近世代数 (H) 课堂笔记

涂嘉乐 PB23151786

2025 春

前言

本人于 2025 春修读了近世代数 (H)，授课老师为中国科学技术大学数学科学学院的陈小伍教授，课程主页为http://home.ustc.edu.cn/ xwchen/ModernAlgebra.htm，课程计划如下：

(1) 环论、域论（重点：整环、商域与域扩张）

(2) 有限群论（重点：循环群与低阶对称群）

(3) Galois 理论与 Galois 大定理（重点：子域与子群的对应）

本课程主要参考以下书籍

(1) 冯克勤, 李尚志, 章璞.《近世代数引论》（这是课本，但是一般不按课本讲）

(2) M.Artin,《Algebra》

(3) J.Rotman,《Galois Theory》（域论，Galois 理论部分按这本讲）

以下是我的笔记，模版是我自己做的，值得一提的是笔记中仿照老师的板书，引入了 Ex 和 Fact，其中 Ex 是小伍老师上课留的练习，一般来说是补全一些证明过程的 Gap，此外小伍老师还喜欢使用 Fact 来呈现一些事实、结论；除此之外笔记中可能存在一些错误，敬请谅解！

涂嘉乐

2025 年春

目录

第一章 预备知识

§1.1 集合与映射

定义 1.1.1（集合与映射）我们用大写字母 $X, Y, Z \cdots$ 来表示集合，用符号 $\subseteq$ 表示子集，如

$$\varnothing \subseteq X \subseteq X$$

称 f 为由集合 X 到 Y 的映射，是指对每个 $x \in X$ 都有确定方法给出集合 Y 中唯一的对应元素，这个元素也叫做 x 在映射 f 下的像，记作 $f(x)$，映射 f 通常写为

$$\begin{aligned} f : X &\longrightarrow Y \\ x &\longmapsto f(x) \end{aligned}$$

或者 $X \xrightarrow{f} Y$

评价 我们称映射 $f : X \to Y, f' : X' \to Y'$ 相等，是指 $X = X', Y = Y', \forall x \in X, f(x) = f'(x)$

例 1.1 恒等映射：任给集合 X，称

$$\begin{aligned} \mathrm{Id}_X : X &\longrightarrow X \\ x &\longmapsto x \end{aligned}$$

为 X 到自身的恒等映射 (identity)

例 1.2 包含映射：设 $S \subseteq X$，称

$$\begin{aligned} \mathrm{inc} : S &\longrightarrow X \\ s &\longmapsto s \end{aligned}$$

为 X 的子集 S 到 X 的包含映射 (inclusion)

定义 1.1.2（复合映射）设有映射 $X \xrightarrow{f} Y, Y \xrightarrow{g} Z$，则 f, g 的复合映射为

$$\begin{aligned} g \circ f : X &\longrightarrow Z \\ x &\longmapsto g(f(x)) \end{aligned}$$

复合映射满足

(1) 结合律：$h \circ (g \circ f) = (h \circ g) \circ f$

(2) 有单位：对 $\forall f : X \to Y$，都有

$$f \circ \mathrm{Id}_X = f = \mathrm{Id}_Y \circ f$$

定义 1.1.3（单射、满射与双射）设有映射 $f : X \to Y$

(1) 称 f 是单射，若对 $\forall x, x' \in X$，若 $f(x) = f(x')$，则 $x = x'$，记为 $X \xhookrightarrow{f} Y$

(2) 称 f 是满射，若对 $\forall y \in Y, \exists X \in x, \text{s.t. } f(x) = y$，记为 $X \xrightarrow{f} \!\!\!\!\rightarrow Y$

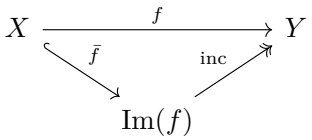
(3) 若 f 既是单射又是满射，则称 f 是双射，记作 $f: X \xrightarrow{\sim} Y$

例 1.3 $\mathrm{Id}_X : X \to X$ 是双射

定义 1.1.4（映射的像）设有映射 $f: X \to Y$，称 $\mathrm{Im}(f) = \{f(x) | x \in X\} \subseteq Y$ 为映射 f 的像

评价 f 是满射 $\iff \mathrm{Im}(f) = Y$

Fact（单满分解）对任意映射 $f: X \to Y$，我们有单满分解（也称典范分解）$f = \mathrm{inc} \circ \bar{f}$，其中 $\bar{f} = f|_X, \mathrm{inc}: \mathrm{Im}(f) \to Y$，即如下交换图成立



评价 上面的 inc 实际上应该写为 $\mathrm{inc}_{\mathrm{Im}(f),Y}$

Ex 设有映射 $f: X \to Y$，求证

(1) f 是单射 $\iff$ 任意两个映射 $g, g': Z \to X$ 满足 $f \circ g = f \circ g'$，则 $g = g'$，即 f 满足左消去律

(2) f 是满射 $\iff$ 任意两个映射 $h, h': Y \to Z$ 满足 $h \circ f = h' \circ f$，则 $h = h'$，即 f 满足右消去律

(3) $f: X \to Y$ 是双射 $\iff \exists g: Y \to X, \text{s.t. } g \circ f = \mathrm{Id}_X, f \circ g = \mathrm{Id}_Y$，且此时 g 是唯一的，记 $g = f^{-1}$，称为 f 的逆

定义 1.1.5（集合的构造）

(1) 无交并：当 $X \cap Y = \varnothing$ 时，记 $X \cup Y \overset{\mathrm{def}}{=} X \sqcup Y$，称为无交并

(2) 笛卡尔积：设 X, Y 是两个集合，定义它们的笛卡尔积为

$$X \times Y = \{(x, y) : x \in X, y \in Y\}$$

其中 $(x, y) = (x', y') \iff x = x', y = y'$

(3) 记 X 到 Y 的全体映射构成的集合为

$$\mathrm{Map}(X, Y) = \{f | f: X \to Y\}$$

(4) 幂集：对任意集合 X，称 X 的子集的全体为 X 的幂集，记为 $\mathcal{P}(X)$

Ex 求证：存在双射 $\mathrm{Map}(X, \{0, 1\}) \xrightarrow{\sim} \mathcal{P}(X)$

Ex 求证：存在双射 $\mathrm{Map}(X \sqcup Y, Z) \xrightarrow{\sim} \mathrm{Map}(X, Z) \times \mathrm{Map}(Y, Z)$

Ex 求证：存在双射 $\mathrm{Map}(X, Y \times Z) \xrightarrow{\sim} \mathrm{Map}(X, Y) \times \mathrm{Map}(X, Z)$

Ex（伴随）求证：存在双射 $\mathrm{Map}(X \times Y, Z) \xrightarrow{\sim} \mathrm{Map}(X, \mathrm{Map}(Y, Z))$

§1.2 等价关系

定义 1.2.1（等价关系与等价类）设 X 是集合，定义 X 上的等价关系 $R \subseteq X \times X$（也记作 $\overset{R}{\sim}$），它满足如下三条性质

(1) 自反性：$(x,x) \in R, \forall x \in X \quad (x \overset{R}{\sim} x)$

(2) 对称性：$(x,y) \in R \Longrightarrow (y,x) \in R \quad (x \overset{R}{\sim} y \Longrightarrow y \overset{R}{\sim} x)$

(3) 传递性：$(x,y),(y,z) \in R \Longrightarrow (x,z) \in R \quad (x \overset{R}{\sim} y, y \overset{R}{\sim} z \Longrightarrow x \overset{R}{\sim} z)$

对 $\forall a \in X$，称

$$[a] = \{x \in X | x \overset{R}{\sim} a\}$$

为 $[a]$ 所在的等价类

例 1.4 最小的等价关系：$\triangle = \{(x,x) | x \in X\} \subseteq X \times X$，不难看出 $\overset{\triangle}{\sim}$ 就是等号

例 1.5 $\mathbb{Z}$ 上模 3 同余关系：$R = \{(m,n) \in \mathbb{Z} \times \mathbb{Z} : 3 \mid m-n\}$，实际上

$$m \overset{R}{\sim} n \iff m \equiv n \mod 3$$

Fact 设 X 上有等价关系 $\overset{R}{\sim}$，则

(1) 对 $\forall b \in [a]$，有 $[b] = [a]$，因此称 $[a]$ 中的任一元素为它的代表元

(2) $[a] \cap [a'] \neq \varnothing \iff [a] = [a']$

Ex 证明上述事实

定义 1.2.2（商集与商映射）设 X 上有等价关系 $\overset{R}{\sim}$，定义商集

$$X/\overset{R}{\sim} \overset{\text{def}}{=} \{\text{等价类全体}\} \subseteq \mathcal{P}(X)$$

进而有商映射（它是满射）

$$\begin{aligned} \pi_R : X &\longrightarrow X/\overset{R}{\sim} \\ a &\longmapsto [a] \end{aligned}$$

定义 1.2.3（完全代表元系）关于等价关系 $\overset{R}{\sim}$ 的完全代表元系（简记为完系）是指 $S \subseteq X$，它满足 $\forall x \in X$，存在唯一 $s \in S, \text{s.t. } [s] = [x]$

例 1.6 记 R 为 $\mathbb{Z}$ 上的模 3 同余关系，则 $\mathbb{Z}/\overset{R}{\sim} = \{[0],[1],[2]\} \overset{\text{def}}{=} \mathbb{Z}_3$，且 $S = \{0,1,2\}, S' = \{-1,0,1\}$ 均为完全代表元系

Fact 设 X 上有等价关系 $\overset{R}{\sim}$

(1) 若 $S \subseteq X$ 为完系，则存在 $S \to X/\overset{R}{\sim}$ 的双射 $\pi_R \circ \text{inc}$，具体如下

$$\begin{aligned} S &\xrightarrow{\text{inc}} X \xrightarrow{\pi_R} X/\overset{R}{\sim} \\ s &\longmapsto s \longmapsto [s] \end{aligned}$$

(2) 此时我们有

$$X = \bigsqcup_{s\in S}[s]$$

定义 1.2.4（分拆）集合 X 的分拆是指 $P = \{X_i : i \in I\} \subseteq \mathcal{P}(X)$，其中 I 是指标集，满足

(1) $X_i \neq \varnothing, \forall i \in I$

(2) $X_i \cap X_j = \varnothing, \forall i \neq j$

(3) $X = \bigsqcup_{i\in I} X_i$

Fact 存在双射

$$\{X\text{上的等价关系}\} \overset{1:1}{\longleftrightarrow} \{X\text{上的分拆}\}$$
$$\overset{R}{\sim} \longmapsto X/\overset{R}{\sim}$$
$$\overset{P}{\sim} \longleftarrow\!\shortmid P = \{X_i : i \in I\}$$

其中 $\overset{P}{\sim}$ 为等价关系：$x \overset{P}{\sim} y \iff \exists i \in I, \text{s.t. } x, y \in X_i$

Fact 任给映射 $f : X \to Y$，它给出了 X 上的等价关系

$$x \overset{f}{\sim} x' \iff f(x) = f(x')$$

其中 $\forall x \in X$ 的等价类为 $[x] = f^{-1}(f(x))$

定义 1.2.5（原像）考虑映射 $f : X \to Y$，对 $\forall y \in Y$，定义原像为

$$f^{-1}(y) = \{x \in X : f(x) = y\} \subseteq X$$

评价 $f^{-1}(y) \neq \varnothing \iff y \in \mathrm{Im}(f)$

定理 1.2.1（映射基本定理）设 $f : X \to Y$，考虑 $\overset{f}{\sim}$，则 f 诱导双射

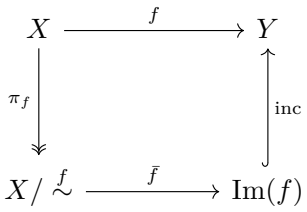
$$\bar{f} : X/\overset{f}{\sim} \longrightarrow \mathrm{Im}(f)$$
$$[x] \longmapsto f(x)$$

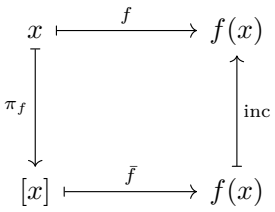
评价 需要验证两点：

(1) $\bar{f}$ 是否良定义 (Well − defined)？即若 $[x] = [x']$，是否有 $f(x) = f(x')$

(2) $\bar{f}$ 是单射？满射？

此外我们有交换图





即 $f = \mathrm{inc} \circ \bar{f} \circ \pi_f$

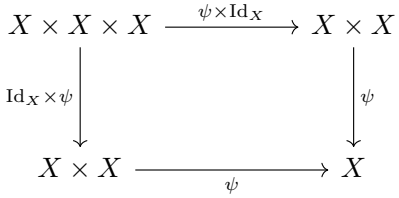
Ex 假设还存在 $h : X/\overset{f}{\sim} \to \mathrm{Im}(f)$ 满足 $f = \mathrm{inc} \circ h \circ \pi_f$，则 $h = \bar{f}$

定义 1.2.6（二元运算）对任意非空集合 X，定义其上的二元运算

$$\begin{aligned} \psi : X \times X &\longrightarrow X \\ (x, y) &\longmapsto \psi(x, y) \in X \end{aligned}$$

称这个二元运算 ψ 满足结合律是指：$\forall x, y, z \in X, \psi(\psi(x, y), z) = \psi(x, \psi(y, z))$

评价 有时我们略去 ψ，用一般的乘法表示，记 $\psi(x, y) = x \cdot y$，则结合律表示为 $(x \cdot y) \cdot z = x \cdot (y \cdot z)$，即括号可以随意添加！二元运算满足结合律当且仅当下面的交换图成立



第二章 环

§2.1 基本概念

定义 2.1.1（环）环是一个非空集合 R 和 R 上两个二元运算（通常表示为 $+,\cdot$）组成的代数结构 $(R,+,\cdot)$，它满足八条公理

(A1) 加法结合律：$\forall a,b,c\in R,(a+b)+c=a+(b+c)$

(A2) 加法交换律：$\forall a,b\in R,a+b=b+a$

(A3) 有零元：$\exists 0_R\in R$，满足对 $\forall a\in R,a+0_R=0_R+a=a$

(A4) 有负元：对 $\forall a\in R,\exists b\in R,\text{s.t. } a+b=0_R=b+a$

(M1) 乘法结合律：$\forall a,b,c\in R,(a\cdot b)\cdot c=a\cdot(b\cdot c)$

(M2) 有幺元：$\exists 1_R\in R$，满足对 $\forall a\in R,a\cdot 1_R=a=1_R\cdot a$

(D1) 左分配律：$\forall a,b,c\in R,(a+b)\cdot c=a\cdot c+b\cdot c$

(D2) 右分配律：$\forall a,b,c\in R,a\cdot(b+c)=a\cdot b+a\cdot c$

评价 (1) 本课程只考虑含幺环，即默认含幺

(2) 可将 $(R,+,\cdot)$ 简记为 R

(3) 两个环 $(R,+,\cdot)$ 和 $(R',\oplus,\otimes)$ 相等当且仅当 $R=R',+=\oplus,\cdot=\otimes$

Fact 零元、负元唯一！

证明 只证明零元唯一，负元唯一性类似：假设还存在一个零元 $0'_R$，则

$$0'_R=0'_R+0_R=0_R+0'_R=0_R$$

□

Ex 证明 $-0_R=0_R,-(-a)=a,\forall a\in R$

例 2.1（环的例子）

(1) 整数环 $\mathbb{Z}=(\mathbb{Z},+\cdot),0_{\mathbb{Z}}=0,1_{\mathbb{Z}}=1$

(2) Gauss 整数环 $\mathbb{Z}[i]=\{m+ni|m,n\in\mathbb{Z}\}\subseteq\mathbb{C}$

(3) 有理系数一元多项式环 $\mathbb{Q}[x]=\{\text{系数为有理数的多项式}\}$

(4) 模 n 同余类环 $\mathbb{Z}_n=\{\overline{0},\overline{1},\cdots,\overline{n-1}\}$，其中零元为 $\overline{0}$，幺元为 $\overline{1}$，加法与乘法定义为

$$\overline{a}+\overline{b}=\overline{a+b},\quad \overline{a}\cdot\overline{b}=\overline{ab}$$

(5) $\mathbb{C}$ 上的全矩阵环 $\mathrm{M}_n(\mathbb{C})=\{n\times n\text{阶复方阵全体}\}$，零元为 $\mathbf{0}_{n\times n}$，幺元为 I_n，它是含幺非交换环

Ex 验证模 n 同余类环中加法与乘法的良定性

评价 设 k 是域，k 上的线性空间 V 也有两种二元运算，即加法和数乘，也满足八条公理，但是与环不同！

命题 2.1.1（环的基本性质）

(1) $\forall a \in R, -(-a) = a$

(2) 加法消去律：$a + b = a + c \Longrightarrow b = c$

Proof : $(-a) + (a + b) = (-a) + (a + c) \Longrightarrow [(-a) + a] + b = [(-a) + a] + c \Longrightarrow b = c$

(3) 定义减法：$a - b \overset{\text{def}}{=} a + (-b)$

(4) 定义倍数：$\forall a \in R, n \in \mathbb{Z}$，定义 a 的 n 倍为 na，对 $\forall n \in \mathbb{Z}$ 有

$$na = \begin{cases} 0_R, & n = 0 \\ \overbrace{a + \cdots + a}^{n\text{个}}, & n > 0 \\ \overbrace{(-a) + \cdots + (-a)}^{-n\text{个}}, & n < 0 \end{cases}$$

(5) 引入求和符号 $\sum\limits_{i=1}^{n} a_i = a_1 + \cdots + a_n$

Ex 试证明

(1) $\forall m, n \in \mathbb{Z}, a \in R$，有 $(m + n)a = ma + na$

(2) $\forall n \in \mathbb{Z}, a \in R$，有 $na = (n1_R) \cdot a = a \cdot (n1_R)$，特别地当 $n = 0$ 时有 $0_R = 0_R \cdot a, \forall a \in R$

(3) $\forall a, b \in R, n \in \mathbb{Z}$，有 $a \cdot (nb) = n(a \cdot b) = (na) \cdot b$

Ex 证明广义分配律：对 $\forall m, n \geq 1$

$$\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{j=1}^{m} b_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{m}(a_i \cdot b_j)$$

命题 2.1.2（零环的等价命题）设 R 为含幺环，则以下命题等价 TFAE(The following are equivalent)

(1) $0_R = 1_R$

(2) $R = \{0_R\}$

(3) R 仅有一个元素

证明 $(2) \Longrightarrow (3), (3) \Longrightarrow (1)$ 都是显然的，下面证明 $(1) \Longrightarrow (2)$：对 $\forall a \in R$，下证 $a = 0_R$

$$a = 1_R \cdot a \overset{(1)}{=} 0_R \cdot a = 0_R$$

□

评价 在后续课程中，除非特殊说明，我们考虑非零环

例 2.2 二元环 $R = \{0_R, 1_R\}$，我们断言 $1_R + 1_R = 0_R$，因为若 $1_R + 1_R = 1_R$，由加法消去律知 $1_R = 0_R$，但它不是零环，矛盾！二元环的加法、乘法表如下

$+$	0_R	1_R
0_R	0_R	1_R
1_R	1_R	0_R

$\cdot$	0_R	1_R
0_R	0_R	0_R
1_R	0_R	1_R

在同构意义下，二元环只有一种，即为 $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$

以下我们考虑含幺交换环

定义 2.1.2（幂次）对 $\forall a \in R, n \in \mathbb{N}$，定义 a 的幂次

$$a^0 = 1_R, \quad a^n = \overbrace{a \cdot a \cdots a}^{n个}, \forall n \geq 1$$

定理 2.1.1（二项式定理）对 $\forall a, b \in R, \forall n \in \mathbb{N}^*$，有

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$$

Ex 证明二项式定理

定义 2.1.3（乘法可逆元） $\forall a \in R$ 称为乘法可逆元（也称单位 ,unit），若 $\exists b \in R$，使得

$$a \cdot b = 1_R = b \cdot a$$

此时记 $b = a^{-1}$

Fact 逆元唯一，且根据定义有 $(a^{-1})^{-1} = a$

例 2.3 $1_R^{-1} = 1_R$，在非零环中，0_R 不可逆！

Fact 可逆元具有乘法消去律：若 $a \in R$ 可逆，且 $a \cdot x = a \cdot y$ 或 $x \cdot a = y \cdot a$，则 $x = y$，因此可逆元具有左/右消去律，可以定义除法：$c \div a = ca^{-1}$

评价 若 a 可逆，则对 $n \geq 1$，可以定义 $a^{-n} \overset{\text{def}}{=} (a^{-1})^n$

定义 2.1.4（单位群）定义环 R 的单位群为

$$U(R) \overset{\text{def}}{=} \{a \in R | a可逆\} \subset R$$

Fact $U(R)$ 有以下性质

(1) R 交换 $\Longrightarrow U(R)$ 是 *Abel* 群
(2) $\pm 1_R \in U(R)$
(3) $a, b \in U(R) \Longrightarrow a \cdot b \in U(R)$
(4) $a \in U(R) \Longrightarrow a^{-1} \in U(R)$

例 2.4 $U(\mathbb{Z}) = \{1, -1\}, U(\mathbb{Q}) = \mathbb{Q}^\times \overset{\text{def}}{=} \mathbb{Q}\backslash\{0\}$

例 2.5 $U(\mathbb{Z}_n) = \{\overline{m} | \gcd(m, n) = 1\}$，如 $U(\mathbb{Z}_8) = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$

定义 2.1.5（整环）称 R 是整环，若 $a \cdot b = 0_R \Longrightarrow a = 0_R$ 或 $b = 0_R$

评价 若 R 是整环，则 $\forall a, b \neq 0_R \Longrightarrow ab \neq 0_R$

例 2.6 (1) $\mathbb{Z}$ 是整环
(2) 当 n 为合数时，$\mathbb{Z}_n$ 不是整环，如在 $\mathbb{Z}_8$ 中有 $\overline{2} \cdot \overline{4} = 0$，但是 $\overline{2}, \overline{4} \neq \overline{0}$

命题 2.1.3 整环有乘法消去律：$\forall a \neq 0_R$，若 $a \cdot b = a \cdot c$，则 $b = c$

证明

$$a \cdot b = a \cdot c \Longrightarrow a \cdot (b - c) = 0_R \overset{a \neq 0_R}{\Longrightarrow} b - c = 0_R \Longrightarrow b = c$$

□

定义 2.1.6（域）称含幺交换环 R 是域，若 $\forall a \neq 0_R$，均有 $a \in U(R)$

Fact 域一定是整环

证明 设 R 是域，对 $\forall a, b \in R\backslash\{0\}$，则 $a, b \in U(R) \Longrightarrow ab \in U(R)$，故 ab 可逆，$ab \neq 0_R$ □

例 2.7 $\mathbb{Q}$ 有理数域；$\mathbb{C}$ 复数域；$\mathbb{Z}, \mathbb{Z}[i]$ 是整环，但不是域

命题 2.1.4 设 $n \geq 2$，则以下命题等价
(1) $\mathbb{Z}_n$ 是整环
(2) n 是素数
(3) $\mathbb{Z}_n$ 是域

证明 (3) $\Longrightarrow$ (1), (1) $\Longrightarrow$ (2) 显然，下面证明 (2) $\Longrightarrow$ (3)：设 $n = p$ 是素数，因为 $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}$，对 $\forall 1 \leq i \leq p - 1$，由于 $(i, p) = 1$，由 Bezout 等式，存在 $a, b \in \mathbb{Z}, \text{s.t. } ai + bp = 1$，因此

$$ai \equiv 1 \mod p \Longrightarrow \overline{a} \cdot \overline{i} = \overline{1}$$

因此 $\overline{i}^{-1} = \overline{a}$ □

评价 因此，我们记 $\mathbb{Z}_p \overset{\text{def}}{=} \mathbb{F}_p$ (Field)

Ex 证明：设 R 是有限环，则 R 是整环 $\Longleftrightarrow$ R 是域（若 R 为无限环，则改命题不成立，考虑 $\mathbb{Z}, \mathbb{Z}[i]$）

定义 2.1.7（子环）设 $S \subseteq R$，若
(1) $1_R \in S$（与书上不同）
(2) S 对 $+,-,\cdot$ 封闭，即 $\forall a,b \in S, a+b, a-b, a\cdot b \in S$
则称 S 是 R 的子环，注意 S 本身也是环，$0_S = 0_R, 1_S = 1_R$

定义 2.1.8（子域）设 K 是域，子环 $S \subseteq K$ 称为子域，若 $\forall 0_R \neq a \in S$，有 $a^{-1} \in S$（即对 $+,-,\cdot,\div$ 封闭），注意 S 本身也是域

例 2.8 $\mathbb{Z} \overset{\text{子环}}{\subseteq} \mathbb{Q}, \mathbb{Q} \overset{\text{子域}}{\subseteq} \mathbb{R} \overset{\text{子域}}{\subseteq} \mathbb{C}$

例 2.9 (1) $\mathbb{Z}$ 没有真子环
(2) $\mathbb{Q}, \mathbb{F}_p$ 没有真子域

证明 只证明 $\mathbb{Z}$ 没有真子环，其余类似：设 $S \subseteq \mathbb{Z}$ 为子环，则 $1 \in S \Longrightarrow 0 = 1-1, -1 = 0-1 \in S$，进而由倍元的公式知 $\forall n \in \mathbb{Z}, n \in S$，即 $\mathbb{Z} \subseteq S$，故 $S = \mathbb{Z}$ □

Ex 分类 $\mathbb{Q}$ 的子环

例 2.10 记 $\mathbb{Q}(i) = \{a+bi | a,b \in \mathbb{Q}\} \subseteq \mathbb{C}$，试分类 $\mathbb{Q}(i)$ 的子域

解 设 $S \subseteq \mathbb{Q}(i)$ 是子域，我们断言：$S = \mathbb{Q}$ 或 $S = \mathbb{Q}(i)$
Proof Of Claim : 因为 $1 \in S$，同上可知 $\mathbb{Q} \subseteq S$
Case 1. $\mathbb{Q} = S$
Case 2. $\mathbb{Q} \subsetneq S \Longrightarrow \exists a+bi \in S, a,b \in \mathbb{Q}, b \neq 0$，进而 $bi \in S \Longrightarrow i = bi \cdot \frac{1}{b} \in S$，因此 $\forall a,b \in \mathbb{Q}, a+bi \in S$，即 $S = \mathbb{Q}(i)$ □

§2.2 商环与理想

定义 2.2.1（环同态）设 $R = (R,+,\cdot), S = (S,\oplus,\otimes)$ 为两个含幺交换环，定义映射 $\theta : R \to S$，称 θ 为环同态 (Ring homomorphism)，若
(1) 保运算：$\forall a,b \in R, \theta(a+b) = \theta(a) \oplus \theta(b), \theta(a\cdot b) = \theta(a) \otimes \theta(b)$
(2) $\theta(1_R) = 1_S$
若 θ 还是双射，则称 θ 为环同构，记为 $\theta : R \xrightarrow{\sim} S$

命题 2.2.1（环同态的性质）设 $\theta : R \longrightarrow S$ 是环同态，则
(1) $\theta(0_R) = 0_S$
(2) $\theta(a-b) = \theta(a) - \theta(b)$
(3) $\theta(a^m) = \theta(a)^m$

评价 可以理解环同态保代数式：如在 R 中有 $a^3b + 4ab = 5c$，则作用 $\theta : R \to S$ 可得

$$\theta^3(a)\theta(b) + 4\theta(a)\theta(b) = 5\theta(c) \quad \text{in } S$$

例 2.11 证明不存在环同态 $\mathbb{Q} \xrightarrow{\theta} \mathbb{Z}_8$

证明 假设存在，则 $\theta(1) = \overline{1} \Longrightarrow \theta(8) = \overline{8} = \overline{0}$，因此

$$\overline{1} = \theta(1) = \theta(8)\theta(\frac{1}{8}) = \overline{0} \cdot \theta(\frac{1}{8}) = \overline{0}$$

矛盾！ □

Ex 证明不存在环同态 $\mathbb{Z}_8 \xrightarrow{\theta} \mathbb{Q}$

引理 2.2.1 设 $\theta : R \to S$ 为环同态，若 $a \in U(R)$，则 $\theta(a) \in U(S)$，且 $\theta(a)^{-1} = \theta(a^{-1})$

证明 若 $a \in U(R)$，则 $1_S = \theta(1_R) = \theta(aa^{-1}) = \theta(a)\theta(a^{-1})$ □

评价 由上述引理知，给定环同态 $\theta : R \to S$，可以得到单位群间的同态 $\theta|_{U(R)} : U(R) \to U(S)$

Fact 若 $\theta : R \to S$ 为环同构，则 $\theta^{-1} : S \to R$ 也为环同构

证明 首先由 θ 是双射知，θ^{-1} 也为双射，下面证明 θ^{-1} 保运算，因为

$$\theta\big(\theta^{-1}(x+y)\big) = x + y = \theta\big(\theta^{-1}(x)\big) + \theta\big(\theta^{-1}(y)\big) = \theta(\theta^{-1}(x) + \theta^{-1}(y))$$

由 θ 是单射知 $\theta^{-1}(x+y) = \theta^{-1}(x) + \theta^{-1}(y)$，乘法类似证明 □

引理 2.2.2 若 $\theta : R \to S, \varphi : S \to T$ 均为环同态，则 $\varphi \circ \theta : R \to T$ 也是环同态

定义 2.2.2（环的自同构群）称 $\mathrm{Aut}(R) = \{\theta | \theta : R \to R\text{是环的自同构}\}$ 为环 R 的自同构群，乘法即为映射的复合

例 2.12 $\mathrm{Aut}(\mathbb{Z}) = \{\mathrm{Id}_{\mathbb{Z}}\}, \mathrm{Aut}(\mathbb{Q}) = \{\mathrm{Id}_{\mathbb{Q}}\}$

证明 只证明 $\mathrm{Aut}(\mathbb{Z}) = \{\mathrm{Id}_{\mathbb{Z}}\}$，另一式同理：设 $\theta \in \mathrm{Aut}(\mathbb{Z})$，则 $\theta(1) = 1$，进而 $\forall n \in \mathbb{Z}, \theta(n) = n$，故 $\theta = \mathrm{Id}_{\mathbb{Z}}$ □

例 2.13 证明 $\mathrm{Aut}(\mathbb{Z}[i]) = \{\mathrm{Id}_{\mathbb{Z}[i]}, \tau\}$，其中 $\tau : m + ni \mapsto m - ni$，即为求共轭映射

证明 设 $\theta \in \mathrm{Aut}(\mathbb{Z})$，同上可知 $\theta|_{\mathbb{Z}} = \mathrm{Id}_{\mathbb{Z}}$，接下来考虑 $\theta(i)$，因为在 $\mathbb{Z}[i]$ 上有 $i^2 + 1 = 0$，所以 $\theta(i)^2 = -1 \Longrightarrow \theta(i) = \pm i$

Case 1. $\theta(i) = i \Longrightarrow \theta = \mathrm{Id}_{\mathbb{Z}[i]}$

Case 2. $\theta(i) = -i \Longrightarrow \theta = \tau$

Ex 完善上述过程，并证明 $\mathrm{Aut}(\mathbb{Q}[i]) = \{\mathrm{Id}, \tau\}$

Ex 设 $\theta : R \to S$ 是环同构，证明

(1) $a \in U(R) \iff \theta(a) \in U(S)$

(2) 有群同构 $U(R) \xrightarrow{\sim} \theta(S)$

(3) R 是整环 $\iff$ S 是整环

(4) 有群同构 $\mathrm{Aut}(R) \xrightarrow{\sim} \mathrm{Aut}(S)$

例 2.14（特征同态）对任意环 R，存在唯一环同态

$$\begin{aligned} \varphi : \mathbb{Z} &\longrightarrow R \\ n &\longmapsto n1_R \end{aligned}$$

称为特征同态

定义 2.2.3（同态的核）设 $\theta : R \to S$ 为环同态，定义环同态 θ 的核为

$$\mathrm{Ker}(\theta) = \{r \in R | \theta(r) = 0_S\} = \theta^{-1}(0_S) \subseteq R$$

评价 $\mathrm{Ker}(\theta)$ 不是 R 的子环，因为 $\theta(1_R) = 1_S \neq 0_S$，故 $1_R \notin \mathrm{Ker}(\theta)$

Fact (1) $\mathrm{Ker}(\theta)$ 对 $+, -, \cdot$ 封闭

(2) $1_R \notin \mathrm{Ker}(\theta)$

(3) $\forall a \in R, r \in \mathrm{Ker}(\theta)$，有 $ar \in \mathrm{Ker}(\theta)$，这是因为

$$\theta(ar) = \theta(a)\theta(r) = \theta(a) \cdot 0_S = 0_S$$

即 $\mathrm{Ker}(\theta)$ 对“倍元”封闭

定义 2.2.4（理想） $\varnothing \neq I \subseteq R$ 称为环 R 的理想，若

(1) $\forall a, b \in I, a + b \in I$

(2) $\forall a \in I, r \in R, a \cdot r \in I$

记作 $I \lhd R$

评价 $r \in I \Longrightarrow -r = (-1_R) \cdot r \in I$，即 I 对减法封闭

例 2.15（平凡理想） $\{0_R\} \lhd R$, $R \lhd R$

Fact 设 $I \lhd R$，则 $I \neq R \iff 1_R \notin I$（实际上把 1_R 改为任意 $a \in U(R)$ 均对）

证明 ($\Longleftarrow$)：显然

($\Longrightarrow$)：反证，若 $1_R \in I$，则 $\forall a \in R, a = a \cdot 1_R \in I$，故 $R = I$，矛盾！ □

定义 2.2.5（主理想）对 $\forall a \in R$，称

$$(a) = aR = \{ra | r \in R\}$$

为 a 生成的主理想，并称 a 为 (a) 的生成元

引理 2.2.3 R 是域 $\iff$ R 仅有平凡理想

证明 $(\Longrightarrow)$：设 R 是域，$\{0_R\} \subsetneqq I \lhd R$，取 $0 \neq a \in I, \forall r \in R$，有

$$r = (ra^{-1})a \in I \Longrightarrow I = R$$

$(\Longleftarrow)$：对 $\forall 0 \neq a \in R$，则 $\{0_R\} \neq (a)$，而 R 仅有平凡理想，故 $(a) = R$，所以 $\exists b \in R, \text{s.t. } ba = 1_R$，即 a 可逆，由 a 的任意性知 R 是域 □

例 2.16 分类 $\mathbb{Z}$ 的理想

解 首先有平凡理想 $\{0\} = 0\mathbb{Z}, \mathbb{Z}$

***Claim*:** $\forall \{0_R\} \subsetneqq I \lhd \mathbb{Z}, \exists! n > 0, \text{s.t. } I = n\mathbb{Z}$

Proof Of Claim：设 $\{0_R\} \subsetneqq I$，则 $\exists! 0 \neq n_0 \in I, \text{s.t. } |n_0|$ 最小，不妨设 $n_0 > 0$（否则由理想对倍元封闭，考虑 $-n_0$），对于 $\forall m \in \mathbb{Z}$，由带余除法，$\exists q \in \mathbb{Z}, 0 \leq r \leq n_0 - 1, \text{s.t. } m = n_0 q + r$，则 $r = m - n_0 q \in I$，由 n_0 的最小性知 $r = 0$，因此 $m = n_0 q \in n_0\mathbb{Z} \Longrightarrow I \subseteq n_0\mathbb{Z}$，且显然有 $n_0\mathbb{Z} \subseteq I$，故 $I = n_0\mathbb{Z}$

唯一性由 n_0 的最小性保证，综上 $\mathbb{Z}$ 的所有理想为 $\{n\mathbb{Z} | n \in \mathbb{N}\}$ □

Fact 存在双射

$$\begin{aligned} \mathbb{Z}_{\geq 0} &\overset{1:1}{\longleftrightarrow} \{\mathbb{Z}\text{的理想}\} \\ n &\longmapsto n\mathbb{Z} \end{aligned}$$

回忆映射基本定理1.2.1

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle \pi_f}\downarrow & & \uparrow{\scriptstyle \text{inc}} \\ X/\overset{f}{\sim} & \xrightarrow{\bar{f}} & \text{Im}(f) \end{array} \qquad \begin{array}{ccc} x & \xrightarrow{f} & f(x) \\ {\scriptstyle \pi_f}\downarrow & & \uparrow{\scriptstyle \text{inc}} \\ [x] & \xrightarrow{\bar{f}} & f(x) \end{array}$$

假设此时 $X = R, Y = S, \theta : R \to S$ 是环同态，则 $\forall a, b \in R$，有

$$a \overset{\theta}{\sim} b \iff \theta(a) = \theta(b) \iff \theta(b - a) = 0_S \iff b - a \in \text{Ker}(\theta) \iff b \in a + \text{Ker}(\theta)$$

如何理解 $R/\overset{\theta}{\sim} \xrightarrow{\bar{\theta}} \text{Im}(\theta)$ 中 $R/\overset{\theta}{\sim}$ 的结构？实际上 $R/\overset{\theta}{\sim} = \{a + \text{Ker}(\theta) | a \in R\} = \{\text{核的平移}\}$

定义 2.2.6（商环）设 $I \lhd R$，商环 R/I 的定义如下

Step 1. 引入 R 上的关系：模 I 同余

$$\forall a, b \in R, \quad a \equiv b \mod I \iff a - b \in I$$

则模 I 同余是 R 上的一个等价关系

(1) 自反性：$a - a = 0_R \in I \Longrightarrow a \equiv a \mod I$

(2) 对称性：若 $a \equiv b \mod I$，则 $a - b \in I \Longrightarrow b - a \in I \Longrightarrow b \equiv a \mod I$

(3) 传递性：若 $a\equiv b \mod I, b\equiv c \mod I$，则 $a-b, b-c\in I \Longrightarrow a-c=(a-b)+(b-c)\in I \Longrightarrow a\equiv c \mod I$

且 $\forall a\in R$，a 的模 I 同余类为

$$\overline{a}=\{b\in R, a-b\in I\}\overset{\text{def}}{=}a+I$$

Step 2. 定义商集 $R/I\overset{\text{def}}{=}R/\equiv=\{\overline{a}|a\in R\}\subseteq\mathcal{P}(R)$，定义 R/I 上的运算

(1) 加法：$\overline{a}+\overline{b}=\overline{a+b}$

(2) 乘法：$\overline{a}\cdot\overline{b}=\overline{a\cdot b}$

则 $(R/I,+,\cdot)$ 是一个含幺交换环，其中 $0_{R/I}=\overline{0}=0+I=I, -\overline{a}=\overline{-a}$

Ex 验证商集 R/I 中加法、乘法的良定性

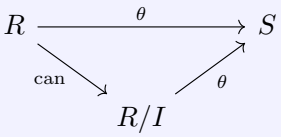
Fact（典范环同态）

$$\begin{aligned}\text{can}: R &\twoheadrightarrow R/I\\ a &\longmapsto \overline{a}\end{aligned}$$

其中 $\text{Ker}(\text{can})=\{a\in R|\overline{a}=\overline{0}\}=I$

例 2.17 设 $n\geq 2$，我们有 $n\mathbb{Z}\lhd\mathbb{Z}$，称 $\mathbb{Z}/n\mathbb{Z}\overset{\text{def}}{=}\mathbb{Z}_n=\{\overline{0},\overline{1},\cdots,\overline{n-1}\}$ 为模 n 同余类环

命题 2.2.2（典范环同态的泛性质）设 $I\lhd R, \text{can}: R\twoheadrightarrow R/I, \theta: R\to S$ 为环同态，满足 $I\subseteq\text{Ker}(\theta)$，则存在唯一环同态 $R/I\overset{\theta'}{\longrightarrow}S, \text{s.t. }\theta=\theta'\circ\text{can}$，用交换图表示为



证明 至多唯一性显然，下证存在性，构造

$$\begin{aligned}\theta': R/I &\longrightarrow S\\ \overline{a} &\longmapsto \theta(a)\end{aligned}$$

则 θ' 是良定的：假设 $\overline{a}=\overline{b}$，则 $a-b\in I\subseteq\text{Ker}(\theta)\Longrightarrow 0_S=\theta(a-b)\Longrightarrow\theta(a)=\theta(b)$

自行验证 θ' 为环同态 □

定理 2.2.1（环同态基本定理）设 $\theta: R\to S$ 是环同态，则存在唯一环同构

$$\begin{aligned}\overline{\theta}: R/\text{Ker}(\theta) &\longrightarrow \text{Im}(\theta)\\ \overline{a} &\longmapsto \theta(a)\end{aligned}$$

即下面的图交换

$$\begin{array}{ccc} R & \xrightarrow{\theta} & S \\ {\scriptstyle \text{can}}\downarrow & & \uparrow{\scriptstyle \text{inc}} \\ R/\mathrm{Ker}(\theta) & \xrightarrow[\overline{\theta}]{} & \mathrm{Im}(\theta) \end{array}$$

证明 由映射基本定理1.2.1知，$\overline{\theta}$ 是双射且唯一，自行验证 $\overline{\theta}$ 为环同态 □

命题 2.2.3 设 $\theta: R \to S$ 为环同态，则

(1) θ 是单同态 $\iff \mathrm{Ker}(\theta) = \{0_R\}$，此时有环同构

$$\begin{aligned} R &\xrightarrow{\sim} \mathrm{Im}(\theta) \\ \theta &\longmapsto \theta(a) \end{aligned}$$

因此我们可以将 R 视为 S 的子环（实际上 $\theta(R)$ 才是 S 的子环），记 $R \overset{\theta}{\hookrightarrow} S$ 为环的嵌入

(2) θ 是满同态 $\iff \mathrm{Im}(\theta) = S$，此时有环同构 $R/\mathrm{Ker}(\theta) \simeq S$，故我们可以将 S 视为 R 的商环

例 2.18（特征同态）

$$\begin{aligned} \varphi: \mathbb{Z} &\longrightarrow R \\ n &\longmapsto n1_R \end{aligned}$$

则 $\exists n_0 \in \mathbb{N}, \text{s.t. } \mathrm{Ker}(\varphi) = n_0\mathbb{Z}$，我们记 $n_0 = \mathrm{Char}(R)$ 为环 R 的特征，特别地

(1) 当 $n = 0$ 时，R 为无限环，可以验证 φ 为单射，故有环嵌入 $\mathbb{Z} \hookrightarrow R$

(2) 当 $n \geq 2$ 时，有环嵌入 $\mathbb{Z}/n\mathbb{Z} \hookrightarrow R$，具体为

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} &\hookrightarrow R \\ \overline{m} &\longmapsto m1_R \end{aligned}$$

Fact 设 R 是整环，则 $\mathrm{Char}(R) = 0$ 或素数

例 2.19 设 $I \subseteq J, I \lhd R, J \lhd R$，则我们有满同态

$$\begin{aligned} \theta: R/I &\twoheadrightarrow R/J \\ a + I &\longmapsto a + J \end{aligned}$$

其中 $\mathrm{Ker}(\theta) = \{(a+I) \in R/I | (a+J) = 0_{R/J}\} = \{(a+I) \in R/I | a \in J\} \overset{\text{def}}{=} J/I$，因此 $J/I \lhd R/I$，由环同态基本定理，存在环同构

$$\begin{aligned} (R/I)/(J/I) &\xrightarrow{\sim} R/J \\ (a+I) + J/I &\longmapsto a + J \end{aligned}$$

定理 2.2.2（对应定理）给定 $I \lhd R$，则存在双射

$$\begin{aligned} \{J \lhd R | I \subseteq J \subseteq R\} &\xleftrightarrow{1:1} R/I\text{的理想} \\ J &\longmapsto J/I = \{\overline{a} = a + I | a \in J\} \\ \{a \in R, \overline{a} \in U\} &\longmapsto U \lhd R/I \end{aligned}$$

Ex 证明对应定理

Ex 分类 $\mathbb{Z}/n\mathbb{Z}$ 的理想（提示：利用对应定理）

Ex 设 R 是环，$S \subseteq R$ 为子环，$I \lhd R$，证明

(1) $S + I = \{a + x | a \in S, x \in I\}$ 为 R 的子环

(2) $(S \cap I) \lhd S$

(3) 有环同构 $S/(S \cap I) \xrightarrow{\sim} (S + I)/I$

Ex（子环版本的对应定理）设 $I \lhd R$，则存在双射

$$\begin{aligned} \{S \subseteq R | I \subseteq S\} &\longrightarrow \{R/I\text{的子环}\} \\ S &\longmapsto S/I \end{aligned}$$

§2.3 分式域与商域

定义 2.3.1（分式域）设 R 是整环，$R^\times = R \backslash \{0\}$，考察 $R \times R^\times = \{(a, x) | a \in R, x \in R^\times\}$，定义 $R \times R^\times$ 上的等价关系

$$(a, x) \simeq (b, y) \iff ay = bx \quad \text{in } R$$

***Claim*:** $\simeq$ 是等价关系

Proof Of Claim : 自反性、对称性显然，下证传递性：设 $(a, x) \simeq (b, y), (b, y) \simeq (c, z)$，则

$$(az)y = (bx)z = (cx)y \Longrightarrow (az - cx)y = 0_R \overset{y \neq 0_R}{\Longrightarrow} az = cx$$

所以 $(a, x) \simeq (c, z)$，我们称 $\simeq$ 对应的等价类为分式，记为

$$\frac{a}{x} = \{(b, y) \in R \times R^\times | (b, x) \simeq (a, x)\}$$

记分式全体 $(R \times R^\times)/\simeq = \mathrm{Frac}(R)$，在 $\mathrm{Frac}(R)$ 上自然定义加法、乘法

$$\begin{cases} \frac{a}{x} + \frac{b}{y} = \frac{ay + bx}{xy} \\ \frac{a}{x} \cdot \frac{b}{y} = \frac{ab}{xy} \end{cases}$$

由下面的练习知 $(\mathrm{Frac}(R), +, \cdot)$ 是域，称为 R 的分式域，其中 $0_{\mathrm{Frac}(R)} = \frac{0_R}{1_R}, 1_{\mathrm{Frac}(R)} = \frac{1_R}{1_R}, -\frac{a}{x} = \frac{-a}{x}$

Ex 验证分式域中加法与乘法的良定性

Fact（典范单同态）

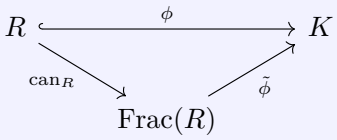
$$\begin{aligned}\mathrm{can}_R : R &\hookrightarrow \mathrm{Frac}(R)\\ a &\longmapsto \frac{a}{1_R}\end{aligned}$$

且我们有同构 $R \simeq \mathrm{Im}(\mathrm{can}_R)$，因此可以将 R 与 $\mathrm{Frac}(R)$ 的子环等同起来

Ex can_R 是同构 $\iff$ R 是域

Fact 设 K, L 是域，且若有同态 $\theta : K \to L$，则 θ 是单射，即域同态一定是单同态

命题 2.3.1（$\mathrm{can}_R : R \hookrightarrow \mathrm{Frac}(R)$ 的泛性质）设 K 是域，则对任意单同态 $\phi : R \hookrightarrow K, \exists! \tilde{\phi} : \mathrm{Frac}(R) \hookrightarrow K$，满足 $\tilde{\phi} \circ \mathrm{can}_R = \phi$，即下面的图交换



特别地，$\tilde{\phi}$ 是同构 $\iff$ $\tilde{\phi}$ 是满射 $\iff$ $\forall w \in K$ 都可表示为 $w = \phi(a)\phi(x)^{-1}, a \in R, x \in R^\times$

证明 至多唯一性：对 $\forall a \in R, x \in R^\times$，因为 $\tilde{\phi} \circ \mathrm{can}_R = \phi$，所以 $\tilde{\phi}(\frac{a}{1_R}) = \phi(a), \tilde{\phi}(\frac{1_R}{x}) = \tilde{\phi}((\frac{x}{1_R})^{-1}) = \tilde{\phi}(\frac{x}{1_R})^{-1} = \phi(x)^{-1}$，因此

$$\forall \frac{a}{x} \in \mathrm{Frac}(R), \quad \tilde{\phi}(\frac{a}{x}) = \tilde{\phi}(\frac{a}{1_R} \cdot \frac{1_R}{x}) = \phi(a)\phi(x)^{-1}$$

即 $\tilde{\phi}$ 的像由 ϕ 唯一决定

存在性：构造

$$\begin{aligned}\tilde{\phi} : \mathrm{Frac}(R) &\longrightarrow K\\ \frac{a}{x} &\longmapsto \phi(a)\phi(x)^{-1}\end{aligned}$$

以上构造是合理的，因为 $x \neq 0_R \overset{\text{单同态}}{\Longrightarrow} \phi(x) \neq 0_R$，且 $\tilde{\phi}$ 是良定的，若 $\frac{a}{x} = \frac{a'}{x'} \iff ax' = a'x$，则

$$\phi(a)\phi(x') = \phi(x)\phi(a') \Longrightarrow \phi(a)\phi(x)^{-1} = \phi(a')\phi(x')^{-1}$$

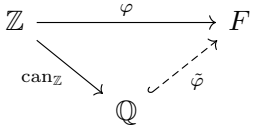
容易验证 $\tilde{\phi}$ 是域同态，且域同态一定是单同态 □

例 2.20 $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$

Ex 证明 $\mathrm{Frac}(\mathbb{Z}[i]) = \mathbb{Q}(i) \overset{\mathrm{def}}{=} \{a + bi | a, b \in \mathbb{Q}\}$

例 2.21 设 F 是域，考虑特征同态 $\varphi : \mathbb{Z} \hookrightarrow F, n \mapsto n1_F$

Case 1. $\mathrm{Char}(F) = 0$，由泛性质2.3.1知



存在唯一的域嵌入

$$\begin{aligned}\tilde{\varphi}:\mathbb{Q}&\hookrightarrow F\\ \frac{m}{n}&\longmapsto (m1_F)(n1_F)^{-1}\end{aligned}$$

此时 F 自然成为 $\mathbb{Q}$-线性空间，数乘定义为

$$\lambda\cdot\boldsymbol{v}=\tilde{\varphi}(\lambda)\boldsymbol{v},\quad \lambda\in\mathbb{Q},v\in F$$

Case 2. $\mathrm{Char}(F)=p$，存在唯一域嵌入

$$\begin{aligned}\tilde{\varphi}:\mathbb{F}_p&\hookrightarrow F\\ \overline{n}&\longmapsto n1_F\end{aligned}$$

则 F 成为 $\mathbb{F}_p$-线性空间，数乘定义为

$$\lambda\cdot\boldsymbol{v}=\tilde{\varphi}(\lambda)\boldsymbol{v},\quad \lambda\in\mathbb{F}_p,v\in F$$

Fact 设 F 为有限域，则存在素数 p 以及正整数 n，使得 $|F|=p^n$

证明 因为 F 是域，所以存在素数 p 使得 $\mathrm{Char}(F)=p$，因此有域嵌入 $\mathbb{F}_p\hookrightarrow F$，进而 F 成为 $\mathbb{F}_p$-线性空间，由线代知识，存在正整数 n 和线性同构

$$F\simeq(\mathbb{F}_p)^d=\mathbb{F}_p\times\cdots\times\mathbb{F}_p$$

□

定义 2.3.2（素理想）称真理想 $p\lhd R$ 为素理想，若 $\forall a\cdot b\in p\Longrightarrow a\in p$ 或 $b\in p$

评价 素理想的等价命题：若 $\forall a,b\notin p$，则 $a\cdot b\notin p$

例 2.22 在 $\mathbb{Z}$ 中，$p\mathbb{Z}\lhd\mathbb{Z}$ 是素理想 $\Longleftrightarrow$ p 是素数

证明 ($\Longrightarrow$)：证明逆否命题，假设 p 不是素数，则 $\exists 1<m,n<p,\text{s.t. }p=mn$，则 $m,n\notin p\mathbb{Z}$，但 $mn\in p\mathbb{Z}$，与 $p\mathbb{Z}$ 是素理想矛盾！

($\Longleftarrow$)：若 $mn\in p\mathbb{Z}$，则 $p\mid mn\Longrightarrow p\mid m,p\mid n\Longrightarrow m\in p\mathbb{Z}$ 或 $n\in p\mathbb{Z}$，故 $p\mathbb{Z}$ 是素理想 □

例 2.23 证明：$\{0_R\}$ 是素理想 $\Longleftrightarrow$ R 是整环

证明 ($\Longrightarrow$) 假设 $ab=0_R$，因为 $\{0_R\}$ 是素理想，所以 $ab\in\{0_R\}\Longrightarrow a\in\{0_R\}$ 或 $b\in\{0_R\}$，即 $a=0_R$ 或 $b=0_R$，进而 $ab=0_R$

($\Longleftarrow$)：留作练习 □

定义 2.3.3（素谱）称

$$\mathrm{Spec}(R)=\{R\text{的全体素理想}\}$$

为环 R 的素谱

例 2.24 $\mathrm{Spec}(\mathbb{Z}) = \{(0), (2), (3), (5), (7), \cdots\}$

定义 2.3.4（极大理想）真理想 $m \lhd R$ 称为极大理想，若 $m \subseteq I \subseteq R$，则 $I = m$ 或 $I = R$

评价 注意素理想和极大理想的前提都是真理想

命题 2.3.2 设真理想 $m \lhd R$，则 m 是极大理想 $\iff$ R/m 是域

证明 一个 non-trivial 的证法：由对应定理知存在一一对应

$$\{I | m \subseteq I, I \lhd R\} \xleftrightarrow{1:1} \{R/m\text{的理想}\}$$

而 $LHS = \{m, R\}$，对应地 $m \mapsto m/m = \{\overline{0}\}, R \mapsto R/m$，故 R/m 只有平凡理想，则 R/m 是域 □

证明（另证）一个比较“土”的证法

$(\Longrightarrow)$: $\forall \overline{0} \neq \overline{a} \in R/m$，若能求出 $\overline{a}^{-1}$，则 R/m 为域，考虑

$$m + (a) = \{x + ar | x \in m, r \in R\} \lhd R$$

则 $m \subseteq m + (a)$，由 m 是极大理想知 $m + (a) = R$，则 $\exists x_0 \in m, r_0 \in R, \text{s.t. } x_0 + ar_0 = 1_R$，所以 $\overline{ar_0} = \overline{1_R}$，故 $\overline{a}^{-1} = \overline{r_0}$

$(\Longleftarrow)$: 留作练习 □

定义 2.3.5（极大谱）称

$$\mathrm{Max}(R) = \{R\text{的全体极大理想}\} \subseteq \mathrm{Spec}(R)$$

为环 R 的极大谱

Fact 设 R 是含幺交换环，则 $\mathrm{Max}(R) \neq \varnothing$，这点由 Zorn 引理保证，承认即可，不要求掌握

例 2.25 $\mathrm{Max}(\mathbb{Z}) = \{(2), (3), (5), (7), \cdots\} \Longrightarrow \mathrm{Spec}(\mathbb{Z}) = \{(0)\} \sqcup \mathrm{Max}(\mathbb{Z})$，且 $\mathbb{Z}$ 的极大理想分别对应了商域 $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_5, \mathbb{F}_7, \cdots$

定义 2.3.6（环中的整除）设 R 是整环，$a \neq 0_R$，约定 $a \mid b \iff b \in (a) \iff \exists r \in R, \text{s.t. } b = ar$

定义 2.3.7（素元）设 $0_R \neq a \in R$，若 $(a) \in \mathrm{Spec}(R)$，即 (a) 为素理想，则称 a 为素元

评价 (1) 素元不可逆（否则 $(a) = R$）

(2) 设 a 非零非单位，则 a 是素元 $\iff$ $a \mid xy$ 能推出 $a \mid x$ 或 $a \mid y$

例 2.26 $\mathbb{Z}$ 中的素元为 $\{\pm 2, \pm 3, \pm 5, \pm 7, \cdots\}$

定义 2.3.8（不可约元）非零非单位元素 $a \in R$ 称为不可约元，若 $a = bc$，则 $b \in U(R)$ 或 $c \in U(R)$，即 a 只有平凡分解 $a = (au^{-1})u, u \in U(R)$

Fact 整环中素元总是不可约元

证明 设 a 是素元，则 $a \neq 0_R, a \notin U(R)$，假设 $a = bc$，则 $a \mid b \cdot c$，由 a 是素元知 $a \mid b$ 或 $a \mid c$，不妨设 $a \mid b$，则 $\exists x \in R, \text{s.t. } b = ax$，所以 $a = axc \overset{\text{整环}}{\Longrightarrow} xc = 1_R$，故 $c = U(R)$，所以 a 只有平凡分解，a 是不可约元 □

例 2.27 $\mathbb{Z}$ 中不可约元和素元等价

Ex 考虑 $\mathbb{Z}[\sqrt{-3}] = \{m + n\sqrt{-3} | m, n \in \mathbb{Z}\}$，证明

(1) $2 \in \mathbb{Z}[\sqrt{-3}]$ 不可约

(2) 2 不是素元

§2.4 一元多项式环

定义 2.4.1（多项式）设 R 是整环，x 是字母，R 上关于 x 的（形式）多项式如下

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

其中 $a_i \in R, \forall i$，$a_n x^n$ 称为 $f(x)$ 的首项，a_n 为首项系数，a_0 为 $f(x)$ 的常数项，并记 $\deg(f(x)) = n$ 为 $f(x)$ 的次数；两个多项式相等当且仅当它们的对应系数均相等

评价 我们约定 $x^0 = 1_R, 1_R x^i = x^i, -1_R x^i = -x^i$；$0_R x^i$ 可以略去

例 2.28 零多项式 $f(x) = 0_R$，我们不规定零多项式的次数；常值多项式 $f(x) = a_0$，若 $a_0 \neq 0$，则 $\deg(f(x)) = 0$；首一多项式 $f(x)$ 的最高次系数 $a_n = 1_R$

命题 2.4.1 记 R 上的多项式全体为

$$R[x] = \{f(x) | f(x) \text{的系数} a_i \in R, \forall i\}$$

在 $R[x]$ 上定义加法与乘法如下：若 $f(x) = \sum\limits_{i=1}^{n} a_i x^i, g(x) = \sum\limits_{j=1}^{m} b_j x^j$，则

$$\begin{cases} f(x) + g(x) = \sum\limits_{l=0}^{\max\{m,n\}} (a_l + b_l) x^l \\ f(x)g(x) = \sum\limits_{l=0}^{m+n} c_l x^l, \quad c_l = \sum\limits_{i=0}^{l} a_i b_{l-i} \end{cases}$$

则 $(R[x], +, \cdot)$ 自然成环，称为 R 上的一元多项式环

评价 上述定义的加法与乘法中，若下标超出，则规定为零，比如 $f(x) = \cdots + 0_R x^{n+1} + a_n x^n + \cdots + a_1 x + a_0$

例 2.29（典范环嵌入）

$$\begin{aligned} R &\hookrightarrow R[x] \\ a &\longmapsto a \end{aligned}$$

其中 $a \in R[x]$ 是常值多项式 $f(x) = a$，因此我们可以将 R 视为 $R[x]$ 的子环

命题 2.4.2 若 R 是整环，则 $R[x]$ 是整环

证明 若 $f(x) = a_n x^n + \cdots + a_1 x + a_0, g(x) = b_m x^m + \cdots + b_1 x + b_0, a_n, b_m \neq 0$，则 $f(x)g(x) = a_n b_m x^{m+n} + \cdots \neq 0$，所以 $R[x]$ 是整环 □

由上述命题的证明过程，我们可以得到

命题 2.4.3 设 R 是整环，$f(x), g(x) \neq 0_R$，则

$$\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$$

命题 2.4.4（多项式环的泛性质）设 R 是环，$\psi : R \to S$ 是环同态，对 $\forall s \in S$，存在唯一环同态 $\tilde{\psi} : R[x] \to S$ 满足

(1) $\tilde{\psi}|_R = \psi$

(2) $\tilde{\psi}(x) = s$

证明 至多唯一性：因为 $\tilde{\psi}(x) = s$，所以 $\tilde{\psi}(x^i) = s^i, \forall i \in \mathbb{N}$，则

$$\tilde{\psi}(a_n x^n + \cdots + a_1 x + a_0) = \psi(a_n)s^n + \cdots + \psi(a_1)s + \psi(a_0)$$

即 $\forall f(x) \in R[x]$ 在 $\tilde{\psi}$ 的像由 ψ 和 s 决定

存在性：验证上述的 $\tilde{\psi}$ 为环同态，留作练习 □

例 2.30（赋值同态）考虑 $\mathrm{Id}_R : R \to R$，任给 $a \in R$，由泛性质2.4.4知，存在唯一环同态

$$\begin{aligned} \mathrm{ev}_a : R[x] &\longrightarrow R \\ x &\longmapsto a \\ \forall r &\longrightarrow r \end{aligned}$$

称为 a 处的赋值同态，设 $f(x) = a_n x^n + \cdots + a_1 x + a_0$，则

$$\mathrm{ev}_a(f(x)) = a_n a^n + \cdots + a_1 a + a_0 \overset{\text{def}}{=} f(a)$$

称 $f(a)$ 为 $f(x)$ 在 $x = a$ 处的取值，$f(a) \in R$

评价 $f(a)$ 是一个“危险”的记号！

命题 2.4.5（余数定理）对 $\forall f(x) \in R[x], a \in R$，则 $\exists q(x) \in R[x]$，使得

$$f(x) = q(x)(x-a) + f(a)$$

证明 因式分解

$$\begin{aligned} f(x) - f(a) &= (a_n x^n + \cdots + a_1 x + a_0) - (a_n a^n + \cdots + a_1 a + a_0) \\ &= (x-a)q(x) \end{aligned}$$

□

Ex 证明 $\mathrm{Ker}(\mathrm{ev}_a) = (x-a)$，其中 $(x-a)$ 表示由 $f(x) = x - a$ 生成的理想

Ex 设 X 是集合，R 是含幺交换环，考虑 $\mathrm{Map}(X,R) = \{\theta : X \to R\text{映射}\}$，定义 $\mathrm{Map}(X,R)$ 上的加法、乘法如下：对 $\forall \delta, \theta \in \mathrm{Map}(X,R)$

$$\begin{aligned} \theta + \delta : X &\longrightarrow R \\ x &\longmapsto \theta(x) + \delta(x) \end{aligned} \qquad \begin{aligned} \theta \cdot \delta : X &\longrightarrow R \\ x &\longmapsto \theta(x) \cdot \delta(x) \end{aligned}$$

证明 $(\mathrm{Map}(X,R), +, \cdot)$ 是含幺交换环

Fact 对 $\forall g(x) \in R[x]$，它决定了一个多项式函数

$$\begin{aligned} g : R &\longrightarrow R \\ a &\longmapsto g(a) \end{aligned}$$

其中 $g(a) = \mathrm{ev}_a(g(x))$，因此 $g \in \mathrm{Map}(R,R)$

Ex 考虑映射

$$\begin{aligned} \mathrm{ev} : R[x] &\longrightarrow \mathrm{Map}(R,R) \\ g(x) &\longmapsto \text{多项式函数} g \end{aligned}$$

证明 ev 是环同态

Ex 在上一个练习中，取 $R = \mathbb{F}_2$，证明

(1) ev 是满射

(2) $\mathrm{Ker}(\mathrm{ev}) = (x^2 + x)$

(3) $\mathrm{Map}(\mathbb{F}_2, \mathbb{F}_2)$ 不是整环

以下考虑 k 是域，对 $\forall f(x) = a_n x^n + \cdots + a_1 x + a_0 \in k[x], a_n \neq 0$，由于域上非零元均可逆，故有

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 = a_n(x^n + a_n^{-1} a_{n-1} x^{n-1} + \cdots + a_n^{-1} a_1 x + a_n^{-1} a_0) = a_n \tilde{f}(x)$$

此时 $f, \tilde{f}$ 生成的主理想是相同的，即 $(f(x)) = (\tilde{f}(x))$，因此我们可以将 $f(x)$ 首一化，且首一化的过程中并未损失任何信息，所以接下来我们可以不妨假设 $f(x)$ 是首一多项式

Key Fact ($k[x]$ 中有带余除法) 设 $f(x)\in k[x], 0\neq g(x)\in k[x]$，用 $g(x)$ 除 $f(x)$ 可得唯一的多项式 $q(x),r(x)\in k[x]$，满足

$$f(x)=q(x)g(x)+r(x)$$

且 $r(x)=0$ 或 $\deg(r(x))<\deg(g(x))$

证明 (带余除法的唯一性) 假设 $f(x)=q(x)g(x)+r(x)=q'(x)g(x)+r'(x)$，则

$$[q(x)-q'(x)]g(x)=r'(x)-r(x)$$

比较次数知 $r'(x)=r(x), q'(x)=q(x)$ □

例 2.31 取 $k=\mathbb{F}_2, f(x)=x^4+x^3+x^2+x+\overline{1}, g(x)=x^2+\overline{1}$，则

$$f(x)=(x^2+x)g(x)+\overline{1}$$

其中 $q(x)=x^2+x, r(x)=\overline{1}$，具体可用长除法求解，我打不出来

评价 $g(x)\mid f(x)\iff r(x)=0_k$

评价 取 $g(x)=x-a$ 即为余数定理2.4.5，进而 $(x-a)\mid f(x)\iff f(a)=0_k$

定义 2.4.2 (根集) 定义 $f(x)$ 在域 k 上的根集为

$$\mathrm{Root}_k(f)=\{a\in k|f(a)=0_k\}$$

定义 2.4.3 (主理想整环,PID) 整环 R 称为 PID (principal ideal domain)，若 $\forall I\lhd R$ 均为主理想，即 $\exists a\in R, \text{s.t. } I=(a)$

评价 因为域只有零理想和本身两个理想，它们可以表示为 $(0),(1)$，所以域均为主理想整环

定理 2.4.1 $\mathbb{Z}, k[x]$ 都是主理想整环

证明 下证 $k[x]$ 是主理想整环，$\mathbb{Z}$ 完全类似!

设 $\{0\}\neq I\lhd k[x]$，取 $h(x)\in I, \text{s.t. } \deg(h(x))$ 最小，我们断言：$(h(x))=I$

Proof Of Claim : 一方面由理想的性质显然有 $(h(x))\subseteq I$，另一方面，对 $\forall f(x)\in I$，由带余除法知

$$f(x)=q(x)h(x)+r(x),\quad q(x),r(x)\in k[x], \deg(r(x))<\deg(h(x))$$

但是 $r(x)=f(x)-q(x)h(x)\in I$, 与 $h(x)$ 次数的最小性矛盾! 所以 $r(x)=0_k$, 即 $f(x)=q(x)h(x)\in(h(x))$ □

定义 2.4.4（最大公因子）设 R 是整环，$a,b\neq 0_R$，定义 a,b 的最大公因子 $\gcd(a,b)\overset{记为}{=}d$ 满足
(1) $d\mid a,d\mid b$
(2) $\forall d'\mid a,d'\mid b$，有 $d'\mid d$

评价 (1) $\gcd(a,b)$ 不一定存在
(2) 若 $\gcd(a,b)$ 存在，则在相伴意义下唯一

定义 2.4.5（相伴）

$$\begin{aligned} a,b\in R\text{相伴} &\iff \exists u\in U(R),\text{s.t. } a=ub\\ &\iff (a)=(b)\\ &\iff a\mid b \text{ 且 } b\mid a\end{aligned}$$

Fact 若 R 是 PID，则对任意非零元 $a,b\in R,\gcd(a,b)$ 存在，且有 Bezout 等式

证明 因为 $(a)+(b)$ 仍为 R 的理想，由 R 是 PID 知，$\exists d\in R,\text{s.t. }(d)=(a)+(b)$，我们断言 $d=\gcd(a,b)$
Proof Of Claim : 因为 $a\in(a)\subseteq(d)\Longrightarrow d\mid a$，同理有 $d\mid b$，且若 $d'\mid a,d'\mid b$，则 $(a)\subseteq(d'),(b)\subseteq(d')$，故有

$$d\in(d)=(a)+(b)\subseteq(d')\Longrightarrow d'\mid d$$

由 $(d)=(a)+(b)$ 知，$\exists u,v\in R,\text{s.t. }d=au+bv$，即为 Bezout 等式 □

评价 $a\mid b\iff(b)\subseteq(a)$，即有一一对应：整除 $\overset{1:1}{\longleftrightarrow}$ 主理想包含

Ex 设 $R=\mathbb{Z}[\sqrt{-3}],a=4,b=(1-\sqrt{-3})^2$，则 $\gcd(a,b)$ 是否存在？

Fact 设 R 是 PID，则 R 不可约元与素元等价

证明 首先整环中素元一定是不可约元，下面证明 PID 中不可约元也是素元：设 $a\neq 0$ 不可约、非单位，设 $a\mid bc,a\nmid b$，则 $\gcd(a,b)=1$，由 *Bezout* 等式，$\exists u,v\in R,\text{s.t. }1=au+bv$，两边同乘 c 得 $c=acu+bcv=a(cu+v)$，故 $a\mid c$，则 a 是素元 □

命题 2.4.6 设 R 是非域的 PID，则

$$\operatorname{Spec}(R)=\{(0)\}\sqcup\operatorname{Max}(R)$$

证明 取 $\{0\}\neq p\in\operatorname{Spec}(R)$，则 $\exists a\in R,\text{s.t. }p=(a)$，且 a 是素元，假设 $p\subseteq I\subsetneq R$，由 R 是 PID 知，$\exists b\in R,\text{s.t. }I=(b)$，进而 $(a)\subseteq(b)\Longrightarrow b\mid a$，由 b 非单位（否则 $(b)=R$）知，a,b 相伴，故 $(b)=(a)$，则 $p=(a)$ 是极大理想 □

定义 2.4.6（最大公因式）设 $k[x]$ 是域上的一元多项式环，我们定义 $\forall f(x), g(x) \in k[x]$ 的最大公因式 $\gcd(f,g) = h(x)$，它满足

$$\begin{cases} h(x) \mid f(x), h(x) \mid g(x) \\ \text{若} a(x) \mid f(x), a(x) \mid g(x)，\text{则} a(x) \mid h(x) \end{cases}$$

我们额外规定 $h(x)$**首一**

评价 我们可以用辗转相除法求 $\gcd(f(x), g(x))$：若 $f(x) = q(x)g(x) + r(x)$，则

$$\gcd(f(x), g(x)) = \gcd(g(x), r(x))$$

对 $q(x), r(x)$ 继续以上操作直到 $r(x) = 0$

定义 2.4.7（不可约多项式） k 上的不可约多项式指的是 $k[x]$ 中的不可约元（或素元）

例 2.32 (1) 在 $\mathbb{C}[x]$ 中，不可约多项式均为一次多项式 $x - a, a \in \mathbb{C}$

(2) $x^2 + 1 \in \mathbb{R}[x]$ 不可约

(3) $x^2 + x + \overline{1} \in \mathbb{F}_2[x]$ 不可约，$x^2 + \overline{1} = (x + \overline{1})^2 \in \mathbb{F}_2[x]$ 可约

评价 由命题2.4.6知

$$\mathrm{Spec}(k[x]) = \{(0)\} \sqcup \mathrm{Max}(k[x])$$

推论 2.4.1 存在一一对应

$$\begin{aligned} k\text{上的首一不可约多项式} &\xleftrightarrow{1:1} \mathrm{Max}(k[x]) \\ f(x) &\longmapsto (f(x)) \end{aligned}$$

特别地有 $k \hookrightarrow \mathrm{Max}(k[x]), \lambda \longmapsto x - \lambda$

定义 2.4.8（域扩张）狭义域扩张：若 k 是 K 的子域，则称 K 是域 k 的扩张，记作 K/k

广义域扩张：若存在域同态（一定是单同态）$\theta : k \hookrightarrow K$，则称域 K 是域 k 的扩张，记作 K/k

评价 广义域扩张中，记 $\mathrm{Im}(\theta) = \theta(k)$，则我们有域同构 $k \xrightarrow{\sim} \theta(k)$，我们将 k 与 $\theta(k)$ 等同，$\theta(k)$ 是 K 的子域；记号 K/k 是危险的记号，它隐藏了 θ 的信息，**真事隐**

Fact 对任意域扩张 $\theta : k \hookrightarrow K$，$K$ 自然成为 k-线性空间，其中数乘定义为

$$\lambda \cdot \boldsymbol{v} = \theta(\lambda) \cdot \boldsymbol{v}, \quad \lambda \in k, \boldsymbol{v} \in K$$

定义 2.4.9（域扩张的维数）设有域扩张 $\theta : k \hookrightarrow K$，定义域扩张 K/k 的维数为 K 做为 k-线性空间的维数，记作 $\dim_k K$ 或 $[K : k]$

评价 设有域扩张 $\theta : k \hookrightarrow K$，它诱导了多项式环同态

$$\begin{aligned} \tilde{\theta} : k[x] &\longrightarrow K[x] \\ f(x) &\longmapsto \tilde{\theta}(f(x)) \end{aligned}$$

其中若 $f(x) = a_n x^n + \cdots + a_1 x + a_0$，则 $\tilde{\theta}(f(x)) = \theta(a_n)x^n + \cdots + \theta(a_1)x + \theta(a_0)$，我们有

(1) $\theta(\mathrm{Root}_k(f)) \subseteq \mathrm{Root}_K(\tilde{\theta}(f))$

(2) $f(x)$ 不可约 $\not\Rightarrow \tilde{\theta}(f(x))$ 不可约

Ex (1) 设 $k \overset{\text{子域}}{\subseteq} K, f(x), g(x) \in k[x] \subseteq K[x]$，证明 $\gcd_{k[x]}(f, g) = \gcd_{K[x]}(f, g)$

(2) 设有域同态 $\theta : k \hookrightarrow K$，将 (1) 推广到一般情况

Kronecker 添根构造

设 $f(x) \in k[x]$ 首一不可约，且 $\deg(f(x)) \geq 2$，则由命题2.3.2知，$K = k[x]/(f(x))$ 是域，对于 $\forall g(x) \in k[x], \overline{g(x)} = g(x) + (f(x)) \in K$，特别地，若 $g(x) = \lambda, \lambda \in k$，则 $\overline{\lambda} = \lambda + (f(x))$，因此有域扩张 $\pi \circ \mathrm{can} : k \hookrightarrow K$，其中 can 为典范单同态，$\pi$ 为商映射

$$\begin{aligned} k \overset{\text{can}}{\hookrightarrow} k[x] &\overset{\pi}{\twoheadrightarrow} K = k[x]/(f(x)) \\ \lambda \longmapsto \quad \lambda \quad &\longmapsto \overline{\lambda} = \lambda + (f(x)) \end{aligned}$$

为方便表示，我们仍然记 $\overline{\lambda} = \lambda$，定义 $\overline{x} = u$，则 K 为 k 线性空间，数乘定义为

$$\lambda \cdot \overline{g(x)} = \overline{\lambda g(x)}$$

为什么称为添根构造？因为当 $n \geq 2$ 时，若 $f(x)$ 不可约，则 $\mathrm{Root}_k(f) = \varnothing$，但是在扩域 $K = k[x]/(f(x))$ 中

$$\overline{0} = \overline{f(x)} = \overline{x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0} = u^n + a_{n-1}u^{n-1} + \cdots + a_1 u + a_0$$

即 $u = \overline{x} \in \mathrm{Root}_K(f)$，这样我们就人为地给 f 添加了一个根！

Key Fact K 有一组 k-基 $\{1, u, \cdots, u^{n-1}\}$，故 $\dim_k K = n$

证明 对 $\forall \overline{g(x)} = k$,在 $k[x]$ 中,对 $g(x)$ 作带余除法 $g(x) = q(x)f(x)+r(x), \deg(r(x)) < \deg(f(x)) = n$，设 $r(x) = c_d x^d + \cdots + c_1 x + c_0, d < n$，则

$$\overline{g(x)} = \overline{r(x)} = \overline{c}_d \cdot \overline{x}^d + \cdots + \overline{c}_1 \cdot \overline{x} + \overline{c}_0 = c_d u^d + \cdots + c_1 u + c_0$$

因此 $\forall \overline{g(x)} \in K$ 均可被 $\{1, u, \cdots, u^{n-1}\}$ 表示，下证它们线性无关，设 $\exists \lambda_0, \cdots, \lambda_{n-1} \in k$，使得

$$\overline{0} = \lambda_{n-1}u^{n-1} + \cdots + \lambda_1 u + \lambda_0 \Longrightarrow \overline{0} = \overline{\lambda_{n-1}x^{n-1} + \cdots + \lambda_1 x + \lambda_0}$$

即在 $k[x]$ 中，$f(x) \mid \lambda_{n-1}x^{n-1} + \cdots + \lambda_1 x + \lambda_0$，由 $f(x)$ 是不可约多项式知，$\lambda_{n-1} = \cdots = \lambda_0 = 0$，因此它们线性无关 □

评价 若为 $\theta: k \hookrightarrow K$，类似上述过程，也可进行添根构造

Ex 若 $\deg(f(x))=1$，即 $f(x)=x-a, a\in k$，则有域同构 $k \xrightarrow{\sim} K=k[x]/(x-a)$

例 2.33 $x^2+1\in\mathbb{R}[x]$ 不可约，则有域扩张 $\mathbb{R}\hookrightarrow K=\mathbb{R}[x]/(x^2+1)$，令 $u=\overline{x}\in K$，则 K 有基 $\{1,u\}$，因为 $u\in \mathrm{Root}_K(x^2+1)$，所以在 K 上有因式分解 $x^2+1=(x+u)(x-u)$，如何在 K 中化简 $(au+b)(cu+d)$？

方法一：因为 $\overline{(ax+b)(cx+d)}=\overline{acx^2+(ad+bc)x+bd}$，由带余除法

$$acx^2+(ad+bc)x+bc=ac(x^2+1)+(ad+bc)x-(bd-ac)$$

所以 $\overline{acx^2+(ad+bc)x+bd}=\overline{(ad+bc)x-(bd-ac)}=(ad+bc)u+(bd-ac)$

方法二：因为在 K 中，$u^2=-1$，所以

$$(au+b)(cu+d)=acu^2+(ad+bc)u+bd=(ad+bc)u+(bd-ac)$$

评价 可以证明 $K\simeq\mathbb{C}$

Ex 求 $K=\mathbb{R}[x]/(x^2+2)$ 的乘法表，问 K 是否与 $\mathbb{C}$ 同构？

例 2.34 考虑 $\mathbb{F}_2=\{\overline{0},\overline{1}\}, x^2+x+\overline{1}\in\mathbb{F}_2[x]$ 不可约，因此有域扩张 $\mathbb{F}_2\hookrightarrow\mathbb{F}_2[x]/(x^2+x+\overline{1})\overset{\text{def}}{=}\mathbb{F}_4$，记 $u=\overline{x}\in\mathbb{F}_4$，则 $\mathbb{F}_4$ 有 $\mathbb{F}_2$-基 $\{\overline{1},u\}$，故

$$\mathbb{F}_4=\{\overline{0},\overline{1},u,u+\overline{1}\}$$

且在 $\mathbb{F}_4$ 中，有 $u^2+u+1=0$，故 $u^2=-u-1=u+1$，我们有如下几点观察

- 求 u^{-1}：$\overline{1}=u(u+\overline{1})$，所以 $u^{-1}=u+\overline{1}$
- 求 u^3：$u^3=u(u^2)=u(u+\overline{1})=u^2+u=\overline{1}$
- 求 $(u+\overline{1})^3$：$(u+\overline{1})^3u^3=(u^2+u)^3=\overline{1}$，所以 $(u+\overline{1})^3=1$
- $<u+\overline{1}>=\{\overline{1},u,u+\overline{1}\}$ 为循环群

上面都是比较取巧的方法，需要极强的注意力，接下来介绍正规做法

- 若要求 $f(u)$，则考虑与 $x^2+x+1\overset{\text{def}}{=}h(x)$ 做带余除法 $f(x)=q(x)h(x)+r(x)$，将 u 代入即得 $f(u)=r(u)$
- 若要求 $f(u)^{-1}$，首先考虑与 $h(x)$ 做带余除法 $f(x)=q(x)h(x)+r(x)$，则 $f(u)=r(u)$，且 $\gcd(r,h)=1$，考虑 $r(x)$ 与 $h(x)$ 的 *Bezout* 等式 $a(x)r(x)+b(x)h(x)=1$，将 u 代入即得 $a(u)r(u)=1$，故 $f(u)^{-1}=r(u)^{-1}=a(u)$

评价 对 $\forall f(x)\in\mathbb{F}_4[x], f+f=\overline{2}f=\overline{0}$

Ex 证明：$\mathbb{F}_4$ 与 $\mathbb{Z}_4$ 不同构

例 2.35 考虑 $\mathbb{F}_3=\{\overline{0},\overline{1},\overline{2}\}, x^2+\overline{1}\in\mathbb{F}_3[x]$ 不可约，因此有域扩张 $\mathbb{F}_3\hookrightarrow\mathbb{F}_3[x]/(x^2+\overline{1})\overset{\text{def}}{=}\mathbb{F}_9$，记 $u=\overline{x}\in\mathbb{F}_9$，则 $\mathbb{F}_9$ 有 $\mathbb{F}_3$-基 $\{\overline{1},u\}$，故

$$\mathbb{F}_9=\begin{Bmatrix}\overline{0} & \overline{1} & \overline{2}\\ u & \overline{1}+u & \overline{2}+u\\ \overline{2}u & \overline{1}+\overline{2}u & \overline{2}+\overline{2}u\end{Bmatrix}$$

且在 $\mathbb{F}_9$ 中，有 $x^2+\overline{1}=(x-u)(x-2u)$，故 $\mathrm{Root}_{\mathbb{F}_9}(x^2+\overline{1})=\{u,\overline{2}u\}$，如何求 $(\overline{1}+\overline{2}u)^{-1}$?

方法一：待定系数法，假设 $(\overline{1}+\overline{2}u)^{-1}=au+b, a,b\in\mathbb{F}_3$，则

$$(au+b)(\overline{1}+\overline{2}u)=\overline{2}au^2+(\overline{2}b+a)u+b=(\overline{2}b+a)u+(b+a)=\overline{1}$$

进而 $\overline{2}b+a=\overline{0}, b+a=\overline{1}$，则 $a=b=\overline{2}$，故 $(\overline{1}+\overline{2}u)^{-1}=\overline{2}+\overline{2}u$

方法二：同例2.34，求 Bezout 等式

Ex 补全上面的 Bezout 等式

Ex 求 $\mathbb{F}_9$ 的乘法表

	$\overline{0}$	$\overline{1}$	$\overline{2}$	u	$\overline{1}+u$	$\overline{2}+u$	$\overline{2}u$	$\overline{1}+\overline{2}u$	$\overline{2}+\overline{2}u$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	u	$\overline{1}+u$	$\overline{2}+u$	$\overline{2}u$	$\overline{1}+\overline{2}u$	$\overline{2}+\overline{2}u$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$	$\overline{2}u$	$\overline{2}+\overline{2}u$	$\overline{1}+\overline{2}u$	u	$\overline{2}+u$	$\overline{1}+\overline{u}$
u	0	u	$\overline{2}u$	$\overline{2}$	$\overline{2}+u$	$\overline{2}+\overline{2}u$	$\overline{1}$	$\overline{1}+u$	$\overline{1}+\overline{2}u$
$\overline{1}+u$	$\overline{0}$	$\overline{1}+u$	$\overline{2}+\overline{2}u$	$\overline{2}+u$	$\overline{2}u$	$\overline{1}$	$\overline{1}+\overline{2}u$	$\overline{2}$	u
$\overline{2}+u$	$\overline{0}$	$\overline{2}+u$	$\overline{1}+\overline{2}u$	$\overline{2}+\overline{2}u$	$\overline{1}$	u	$\overline{1}+u$	$\overline{2}u$	$\overline{2}$
$\overline{2}u$	$\overline{0}$	$\overline{2}u$	u	$\overline{1}$	$\overline{1}+\overline{2}u$	$\overline{1}+u$	$\overline{2}$	$\overline{2}+\overline{2}u$	$\overline{2}+u$
$\overline{1}+\overline{2}u$	$\overline{0}$	$\overline{1}+\overline{2}u$	$\overline{2}+u$	$\overline{1}+u$	$\overline{2}$	$\overline{2}u$	$\overline{2}+\overline{2}u$	u	$\overline{1}$
$\overline{2}+\overline{2}u$	$\overline{0}$	$\overline{2}+\overline{2}u$	$\overline{1}+u$	$\overline{1}+\overline{2u}$	u	$\overline{2}$	$\overline{2}+u$	$\overline{1}$	$\overline{2}u$

表 1: $\mathbb{F}_9$ 的乘法表

评价 思考：$x^2+x+\overline{2}\in\mathbb{F}_3[x]$ 也不可约，同上过程可以得到 $\mathbb{F}_3/(x^2+x+\overline{2})\overset{\text{def}}{=}\mathbb{F}_9$，实际上 $\mathbb{F}_9\simeq\mathbb{F}_9'$

命题 2.4.7（添根构造的泛性质）设 $f(x)\in k[x]$ 不可约，$\theta: k\hookrightarrow K=k[x]/(f(x))$，则任给域同态 $\delta: k\hookrightarrow F$ 以及 $\alpha\in\mathrm{Root}_F(\delta(f))$，则存在唯一域同态 $\delta': K\longrightarrow F$ 满足

(1) $\delta'\circ\theta=\delta$

(2) $\delta'(u)=\alpha$，其中 $u=\overline{x}\in K$

证明 至多唯一性：因为 $\{1,u,\cdots,u^{n-1}\}$ 是 K 的一组 k-基，且

$$\delta'\big(\theta(a_{n-1})u^{n-1}+\cdots+\theta(a_1)u+\theta(a_0)\big)=\delta(a_{n-1})\alpha^{n-1}+\cdots+\delta(a_1)\alpha+\delta(a_0)$$

即 δ' 由 θ,u 唯一确定

存在性：由多项式环的泛性质2.4.4，对 $k\overset{\delta}{\hookrightarrow}F$，存在唯一 $\tilde{\delta}$ 如下

$$\begin{aligned}\tilde{\delta}: k[x]&\longrightarrow F\\ x&\longmapsto\alpha\\ \lambda&\longmapsto\delta(\lambda)\end{aligned}$$

容易验证 $\mathrm{Ker}(\tilde{\delta})=(f(x))$，因此 $\tilde{\delta}$ 诱导环同态

$$\begin{aligned}\delta' : K=k[x]/(f(x)) &\longrightarrow F\\ \overline{g(x)} &\longmapsto \delta(g)(\alpha)\end{aligned}$$

□

例 2.36 考虑两个添根构造 $\theta:\mathbb{F}_3\hookrightarrow \mathbb{F}_9=\mathbb{F}_3[x]/(x^2+\overline{1}), \delta:\mathbb{F}_3\hookrightarrow \mathbb{F}_9'=\mathbb{F}_3[x]/(x^2+x+\overline{2})$，求证 $\mathbb{F}_9\simeq\mathbb{F}_9'$

证明 设 $u=\overline{x}\in\mathbb{F}_9, v=\overline{x}\in\mathbb{F}_9'$，则

$$\mathbb{F}_9=\begin{Bmatrix}\overline{0} & \overline{1} & \overline{2}\\ u & \overline{1}+u & \overline{2}+u\\ \overline{2}u & \overline{1}+\overline{2}u & \overline{2}+\overline{2}u\end{Bmatrix},\qquad \mathbb{F}_9'=\begin{Bmatrix}\overline{0} & \overline{1} & \overline{2}\\ v & \overline{1}+v & \overline{2}+v\\ \overline{2}v & \overline{1}+\overline{2}v & \overline{2}+\overline{2}v\end{Bmatrix}$$

要使用泛性质，我们通过坚持与努力找到 $\alpha\in\mathrm{Root}_{\mathbb{F}_9'}(x^2+\overline{1})=\{v+\overline{2},\overline{2}v+\overline{2}\}$，由泛性质，存在两个域嵌入

$$\begin{aligned}\delta'_{v+\overline{2}}:\mathbb{F}_9&\hookrightarrow\mathbb{F}_9' & \delta'_{\overline{2}v+\overline{1}}:\mathbb{F}_9&\hookrightarrow\mathbb{F}_9'\\ \overline{0},\overline{1},\overline{2}&\longmapsto\overline{0},\overline{1},\overline{2} & \overline{0},\overline{1},\overline{2}&\longmapsto\overline{0},\overline{1},\overline{2}\\ u&\longmapsto v+\overline{2} & u&\longmapsto\overline{2}v+\overline{1}\end{aligned}$$

由它们是单射，且 $|\mathbb{F}_9|=|\mathbb{F}_9'|=9$ 知，它们是满射，故 $\mathbb{F}_9\simeq\mathbb{F}_9'$ □

Ex 考虑 $\mathbb{F}_9''=\mathbb{F}_3[x]/(x^2+\overline{2}x+\overline{2})$，具体构造域同构 $\mathbb{F}_9\xrightarrow{\sim}\mathbb{F}_9''$

§2.5 欧式整环

定义 2.5.1（欧式整环）整环 R 称为欧式整环 (ED)，若存在 size function

$$\begin{aligned}\varphi:R^\times=R\backslash\{0_R\}&\longrightarrow\mathbb{Z}_{\geq 0}\\ a&\longmapsto\varphi(a)\end{aligned}$$

使得任给 $a,b\in R^\times,\exists q,r$ 满足

$$a=qb+r,\quad r=0_R\text{或}\varphi(r)<\varphi(b) \tag{2.1}$$

例 2.37 整数环 $\mathbb{Z}$ 是 ED，它的 size function 为绝对值函数 $\varphi(z)=|z|$，但是表达式 (2.1) 并不唯一，例如

$$33=3\times 9+6=4\times 9+(-3)$$

第二个表达式 $33=4\times 9+(-3)$ 更好，因为 $\varphi(-3)=3$ 更小

例 2.38 域上的一元多项式环 $k[x]$ 是 ED，它的 size function 是求次数 $\varphi(f(x))=\deg(f(x))$

定理 2.5.1 ED 是 PID

证明 设 R 是 ED，对任意非零理想 $I \lhd R$，取非零元 $b \in I, \text{s.t. } \varphi(b)$ 最小（$\varphi(b)$ 不唯一）

***Claim*:** $I = (b)$

Proof Of Claim : 对 $\forall a \in I$，因为 R 是 ED，所以 $\exists q, r \in R, \text{s.t. } a = qb + r$，因为 $r = a - qb \in I$，由 b 的最小性知 $r = 0_R$，进而 $a = qb \in (b)$，故 $I \subseteq (b)$，另一方面显然有 $(b) \subseteq I$，故 $I = (b)$ □

命题 2.5.1 *Gauss* 整数环 $\mathbb{Z}[i]$ 是 ED。进而是 PID

证明 Recall the norm map

$$\begin{aligned} N : \mathbb{Q}(i)^\times &\longrightarrow \mathbb{Q}^\times \\ z &\longmapsto z \cdot \overline{z} \end{aligned}$$

它是积性函数：$N(z_1 z_2) = z_1 z_2 \overline{z}_1 \overline{z}_2 = N(z_1) N(z_2)$，我们将 N 限制在 $\mathbb{Z}[i]^\times$ 上，仍记为 N，则我们断言 $N : \mathbb{Z}[i]^\times \longrightarrow \mathbb{Z}_{\geq 0}$ 就是 size function

Proof Of Claim : 对 $\forall x, y \in \mathbb{Z}[i]^\times$，在 $\mathbb{Q}(i)^\times$ 中，$\exists \alpha, \beta \in \mathbb{Q}, \text{s.t. } \frac{x}{y} = \frac{x\overline{y}}{y\overline{y}} = \alpha + \beta i$，因此 $\exists m, n \in \mathbb{Z}, \text{s.t. } |\alpha - m| \leq \frac{1}{2}, |\beta - n| \leq \frac{1}{2}$，故

$$\frac{x}{y} = \alpha + \beta i = m + ni + (\alpha - m) + (\beta - n)i \overset{\text{def}}{=} q + r'$$

其中 $q = m + ni, r' = (\alpha - m) + (\beta - n)i$，再记 $r = r'y$，则 $x = qy + r$，且

$$N(r) = N(r')N(y) = [(\alpha - m)^2 + (\beta - n)^2]N(y) \leq \left(\frac{1}{4} + \frac{1}{4}\right) N(y) = \frac{1}{2} N(y) < N(y)$$

由 x, y 的任意性知 $\mathbb{Z}[i]$ 是 ED □

评价 可以利用范数映射 N 来证明 $U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$

例 2.39 在 $\mathbb{Z}[i]$ 中求 $\gcd(4 + 7i, 3 + 4i)$

解 辗转相除法

- $\frac{4+7i}{3+4i} = 2 + \left(-\frac{2}{5} + \frac{i}{5}\right) \Longrightarrow 4 + 7i = 2(3 + 4i) + (-2 - i) \Longrightarrow \gcd(4 + 7i, 3 + 4i) = \gcd(3 + 4i, 2 + i)$
- $\frac{3+4i}{2+i} = 2 + i \Longrightarrow \gcd(3 + 4i, 2 + i) = 2 + i$

命题 2.5.2 $\mathbb{Z}[\sqrt{-2}]$ 是 ED，进而是 PID

证明 仍然考虑范数映射限制在 $\mathbb{Z}[\sqrt{-2}]^\times$ 上，仍记为 N

$$\begin{aligned} N : \mathbb{Z}[\sqrt{-2}]^\times &\longrightarrow \mathbb{Z}_{\geq 0} \\ a + b\sqrt{-2} &\longmapsto a^2 + 2b^2 \end{aligned}$$

□

Ex 补全上面的证明

Ex 证明 $(2,1+\sqrt{-3})=(2)+(1+\sqrt{-3})\subseteq\mathbb{Z}[\sqrt{-3}]$ 是素理想，但不是主理想

评价 这个练习说明 $\mathbb{Z}[\sqrt{-3}]$ 不是 PID，进而不是 ED，实际上如果仿照命题2.5.1的证明过程，放缩过程会出现 $\frac{1}{4}+3\cdot\frac{1}{4}=1$，它不严格小于 1，此时范数映射不再是 size function

Ex 考虑三次单位根 $\omega=\frac{-1+\sqrt{-3}}{2},\omega^2+\omega+1=0$，称 $\mathbb{Z}[\omega]=\{m+n\omega|m,n\in\mathbb{Z}\}$ 为 Eisenstein 整数环，证明 $\mathrm{Frac}(\mathbb{Z}[\omega])\simeq\mathbb{Q}(\sqrt{-3})$

评价 $\mathbb{Q}(\sqrt{-3})$ 有两组 $\mathbb{Q}$-基：$\{1,\sqrt{-3}\},\{1,\omega\}$

命题 2.5.3 $\mathbb{Z}[\omega]$ 是 ED，进而是 PID

证明 仍然考虑范数映射限制在 $\mathbb{Z}[\omega]^\times$ 上，仍记为 N

$$\begin{aligned}N:\mathbb{Z}[\omega]^\times&\longrightarrow\mathbb{Z}_{\geq0}\\ a+b\omega&\longmapsto a^2+b^2-ab\end{aligned}$$

□

Ex 补全上面的证明

Ex 证明：

(1) $2\in\mathbb{Z}[\omega]$ 是素元

(2) $U(\mathbb{Z}[\omega])=\{\pm1,\pm\omega,\pm\omega^2\}$

定义 2.5.2（代数整数）考虑 $\mathbb{Z}\subseteq R\subseteq F=\mathrm{Frac}(R)$，且 $\dim_{\mathbb{Q}}F<+\infty$，称 $\alpha\in F$ 为代数整数，若 α 满足首一的整系数方程

$$\alpha^n+a_{n-1}\alpha^{n-1}+\cdots+a_1\alpha+a_0=0,\quad\forall a_i\in\mathbb{Z}$$

我们记 F 中的所有代数整数全体位 $\mathcal{O}_F$

Fact $\mathcal{O}_F\subseteq F$ 是子环，对 $+,-,\cdot$ 封闭，且 $\mathrm{Frac}(O_F)=F$

Ex 设 $F=\mathbb{Q}(\sqrt{-3})$，求证 $\mathcal{O}_F=\mathbb{Z}[\omega]$

评价 $\mathbb{Z}[\omega]$ 是 Dedekind 整环，但 $\mathbb{Z}[\sqrt{-3}]$ 不是 Dedekind 整环

例 2.40 考虑 $\mathbb{Z}(\sqrt{2})=\{m+n\sqrt{2}|m,n\in\mathbb{Z}\}$

Ex 证明

$$\begin{aligned}\sigma:\mathbb{Q}(\sqrt{2})&\longrightarrow\mathbb{Q}(\sqrt{2})\\ a+b\sqrt{2}&\longmapsto a-b\sqrt{2}\end{aligned}$$

是域自同构

Ex 证明 $\mathbb{Z}[\sqrt{2}]$ 是 ED，进而是 PID

Hint：考虑 $N(a+b\sqrt{2})=|(a+b\sqrt{2})\sigma(a+b\sqrt{2})|$

评价 $U(\mathbb{Z}[\sqrt{2}])$ 是无限群

Fact $\mathbb{Z}[\sqrt{3}]$ 是 ED，但 $\mathbb{Z}[\sqrt{5}]$ 不是 ED，$\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ 是 ED

§2.6 高斯整环

目标：研究 $\mathbb{Z}[i]$ 的所有素理想；分类 $\mathbb{Z}[i]$ 中的素元

定义 2.6.1（Gauss 素数） Gauss 整环中的素元称为 Gauss 素数

Fact 设 R 是 PID，回忆相伴的定义2.4.5，我们有一一对应关系

$$\begin{aligned} \{R\text{中的素元}\}/\text{相伴} &\longrightarrow \mathrm{Max}(R) \\ a &\longmapsto (a) \end{aligned}$$

此时 $\mathrm{Spec}(R) = \{(0)\} \sqcup \mathrm{Max}(R)$

引理 2.6.1 对 $\forall m+ni \in \mathbb{Z}[i]$，它与 $-m-ni, -n+mi, n-mi$ 相伴

例 2.41 在 $\mathbb{Z}[i]$ 中，$2 = (1+i)(1-i)$ 与 $(1+i)^2$ 相伴

例 2.42 在 $\mathbb{Z}[i]$ 中，$1+i$ 是素元

证明 首先 $1+i$ 非零非单位，其次在 PID 中素元与不可约元等价，下证 $1+i$ 不可约，假设 $1+i = xy$，利用范数映射 $2 = N(1+i) = N(x)N(y)$，因此一定有 $N(x) = 1$ 或 $N(y) = 1$，故只能是 x 或 y 为单位，即 $1+i$ 只有平凡分解 □

例 2.43 研究 $\mathbb{Z}[i]/(1+i)$

解 因为 $2 = (1+i)(1-i)$，所以 $\overline{2} = 0$，所以 $\forall m+ni \in \mathbb{Z}[i]$，模去 2 得

$$\overline{m+ni} = \begin{cases} \overline{0} \\ \overline{1} \\ \overline{i} \\ \overline{1+i} \end{cases}$$

又因为 $\overline{1+i} = \overline{0}$，$\overline{1-i} = \overline{-i(1-i)} = \overline{1+i} = \overline{0}$，故 $\overline{1} = \overline{i}$，故 $\mathbb{Z}[i]/(1+i) = \{\overline{0}, \overline{1}\} \simeq \mathbb{F}_2$

评价 一些困难的问题往往需要最朴素的分析

Ex 证明：存在群同态 $\phi : \mathbb{Z}[i] \to \mathbb{F}_2, m+ni \mapsto \overline{m+n}$，并证明 $\mathbb{Z}[i]/(1+i) \simeq \mathbb{F}_2$

引理 2.6.2 设 $z \in \mathbb{Z}[i]$，若 $N(z) = p$ 是素数，则 z 是 Gauss 素数

证明 只需证明 z 是不可约元，假设 $z = xy, x, y \in \mathbb{Z}[i]$，则 $p = N(z) = N(x)N(y)$，因为 $N(x), N(y) \in \mathbb{N}$，故必有一个为 1，不妨设 $N(x) = 1$，则 $x \in U(\mathbb{Z}[i])$，故 z 是不可约元 □

引理 2.6.3 设 p 是 $4k+3$ 型素数，则 p 是 Gauss 素数

证明 只需证明 p 不可约，假设有非平凡分解 $p=xy$，则 $p^2=N(p)=N(x)N(y)$，由非平凡分解知 $N(x)=N(y)=p$，假设 $x=m+ni$，则 $N(x)=m^2+n^2=p$，两个整数相加是奇数一定是一奇一偶，不妨设 $m=2i,n=2j+1$，则 $p=m^2+n^2=4i^2+4j^2+4j+1=4(i^2+j^2+j)+1$，与 p 是 $4k+3$ 型素数矛盾！故 p 不可约 □

例 2.44
- $5=1^2+2^2=(1+2i)(1-2i)$
- $13=2^2+3^2=(2+3i)(2-3i)$
- $17=1^2+4^2=(1+4i)(1-4i)$

定理 2.6.1（Fermat 二平方和定理）设 p 为奇素数，则

$$p=4k+1 \iff p=a^2+b^2,\quad a,b\in\mathbb{Z}_{>0}\text{且不计次序下表达唯一}$$

证明 $(\Longleftarrow)$：显然

$(\Longrightarrow)$：***Claim:*** 有环同构

$$\mathbb{Z}[i]/(p)\simeq\mathbb{F}_p[x]/(x^2+\overline{1})$$

Proof Of Claim：Step 1. 首先证明有环同构 $\mathbb{Z}[x]/(x^2+1)\simeq\mathbb{Z}[i]$，考虑多项式环的泛性质2.4.4，存在唯一群同态

$$\begin{aligned}\phi:\mathbb{Z}[x]&\longrightarrow\mathbb{Z}[i]\\ x&\longmapsto i\\ \forall a&\longmapsto a\end{aligned}$$

下证 $\mathrm{Ker}(\phi)=(x^2+1)$，一方面显然有 $(x^2+1)\subseteq\mathrm{Ker}(\phi)$，另一方面，对 $\forall f(x)\in\mathrm{Ker}(\phi)$，则 $f(i)=0$，做带余除法 $f(x)=q(x)(x^2+1)+r(x),\deg(r(x))<\deg(f(x))$，两边同时作用 ϕ 得，$r(i)=0$，但是 x^2+1 为 $\mathbb{Z}[x]$ 上的不可约多项式，故只能是 $r(x)=0$，所以 $f(x)=q(x)(x^2+1)\in(x^2+1)$，故 $\mathrm{Ker}(\phi)=(x^2+1)$，且显然有 ϕ 是满射，由环同态基本定理2.2.1知有环同构

$$\begin{aligned}\tilde{\phi}:\mathbb{Z}[x]/(x^2+1)&\xrightarrow{\sim}\mathbb{Z}[i]\\ \overline{f(x)}&\longmapsto f(i)\end{aligned}$$

Step 2. 对于环同构 $\tilde{\phi}$，有理想对应关系 $(p,x^2+1)/(x^2+1)=(p)/(x^2+1)\xmapsto{\tilde{\phi}}(p)$，由下面的练习知，$\tilde{\phi}$ 诱导同构

$$\Phi:\frac{\mathbb{Z}[x]/(x^2+1)}{(p,x^2+1)/(x^2+1)}\xrightarrow{\sim}\mathbb{Z}[i]/(p)$$

Step 3. 接下来证明有环同构 $\mathbb{Z}[x]/(p)\simeq\mathbb{F}_p[x]$，考虑满同态

$$\begin{aligned}\psi:\mathbb{Z}[x]&\twoheadrightarrow\mathbb{F}_p[x]\\ x&\longmapsto x\\ a&\longmapsto\overline{a}\end{aligned}$$

下面证明 $\mathrm{Ker}(\psi)=(p)$，一方面显然有 $(p)\subseteq\mathrm{Ker}(\psi)$，另一方面对 $\forall f(x)=a_nx^n+\cdots+a_1x+a_0\in\mathrm{Ker}(\psi)$，因为 $\overline{f(x)}\equiv 0$，所以 $\forall i,p\mid a_i$，故 $f(x)\in(p)$，所以 $\mathrm{Ker}(\psi)=(p)$，由环同态基本定理2.2.1知有环同构

$$\begin{aligned}\tilde{\psi}:\mathbb{Z}[x]/(p)&\xrightarrow{\sim}\mathbb{F}_p[x]\\ f(x)+(p)&\longmapsto\overline{f(x)}\end{aligned}$$

Step 4. 对于环同构 $\tilde{\psi}$，有理想对应关系 $(p,x^2+1)/(p)=(x^2+1)/(p)\xmapsto{\tilde{\psi}}(x^2+1)$，故 $\tilde{\psi}$ 诱导同构

$$\Psi:\frac{\mathbb{Z}[x]/(p)}{(p,x^2+1)/(p)}\xrightarrow{\sim}\mathbb{F}_p[x]/(x^2+1)$$

Step 5. 类似例2.19，对 Φ,Ψ 两个同构，我们有

$$\mathbb{Z}[i]/(p)\simeq\frac{\mathbb{Z}[x]/(x^2+1)}{(p,x^2+1)/(x^2+1)}\simeq\mathbb{Z}[x]/(p,x^2+1)\simeq\frac{\mathbb{Z}[x]/(p)}{(p,x^2+1)/(p)}\simeq\mathbb{F}_p[x]/(x^2+1)$$

因此断言得证

又因为 $p=4k+1$，所以 -1 模 p 二次剩余，即 $x^2+\overline{1}=0$ 在 $\mathbb{F}_p[x]$ 中有根，故它在 $\mathbb{F}_p[x]$ 中有因式分解 $x^2+\overline{1}=(x-x_1)(x-x_2),x_1,x_2\in\mathbb{F}_p$，进而 $\overline{x-x_1}\cdot\overline{x-x_2}=\overline{0}$，即 $\mathbb{F}_p[x]/(x^2+1)$ 不是整环，由环同构知 $\mathbb{Z}[i]/(p)$ 不是整环，故 (p) 不是素理想，即 p 在 $\mathbb{Z}[i]$ 中有非平凡分解 $p=xy$，利用范数映射 $p^2=N(x)N(y)$，由非平凡分解知 $N(x)=N(y)=p$，而 p 不是一个整数的平方和，故 $\exists a,b\in\mathbb{Z}\backslash\{0\},\text{s.t. }x=a+bi$，即 $p=N(x)=a^2+b^2$ □

Ex 若 $\theta:R\xrightarrow{\sim}S$ 为环同构，$I\lhd R,\theta(I)\lhd S$，则 $R/I\simeq S/\theta(I)$

评价 从 $\mathbb{Z}[i]/(p)$ 到 $\mathbb{F}_p[x]/(x^2+\overline{1})$ 的同构具体如下

$$\begin{aligned}\mathbb{Z}[i]/(p)&\longrightarrow\mathbb{F}_p[x]/(x^2+\overline{1})\\ \overline{m+ni}&\longmapsto\overline{\overline{m}+\overline{n}x}\end{aligned}$$

定理 2.6.2（Gauss 素数的分类） Gauss 素数在相伴意义下可分为以下三类

(1) $1+i$

(2) 素数 $p=4k+3$

(3) $a\pm bi$，其中 $a^2+b^2=p$ 为 $4k+1$ 型素数

证明 首先由前面的讨论知 (1)(2)(3) 均为 Gauss 素数，且互不相伴，下面证明任意 Gauss 素数都为上述三种中的一种，设 $z\in\mathbb{Z}[i]$ 为 Gauss 素数，在 $\mathbb{Z}$ 中对 $N(z)$ 做素因子分解

$$z\mid z\cdot\overline{z}=N(z)=p_1^{e_1}\cdots p_n^{e_n}$$

注意到每个整素数可以被上述三种数表示

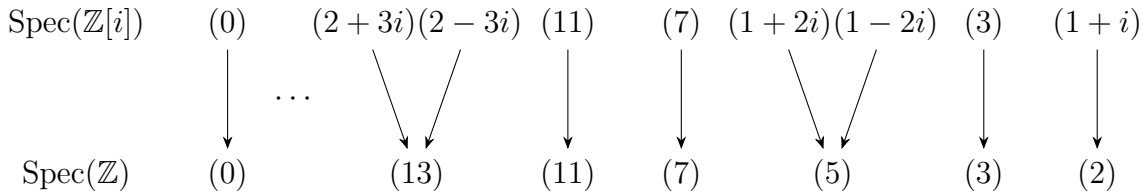
- $2=(1+i)(1-i)$
- $4k+3$ 型素数 $p_i=p_i$
- $4k+1$ 型素数 $p_i=a^2+b^2=(a+bi)(a-bi)$

所以有 $z \mid N(z) = z_1 \cdots z_s$，其中 $\forall i, z_i$ 为 (1)(2)(3) 三种 Gauss 素数，故 $\exists 1 \le i \le s, \text{s.t. } z \mid z_i$，由于 z, z_i 均为 Gauss 素数，故 z, z_i 相伴，故 z 为上述三类中的某一类 □

评价 由 Dirichlet 定理，$4k+1$ 型、$4k+3$ 型素数均匀无穷多个，故 Gauss 素数也有无穷多个

Ex 证明：对 $\forall p \in \text{Spec}(\mathbb{Z}[i])$，则 $(p \cap \mathbb{Z}) \in \text{Spec}(\mathbb{Z})$

例 2.45 由上面的练习，我们可以画出 $\text{Spec}(\mathbb{Z}[i]) \longrightarrow\!\!\!\!\!\rightarrow \text{Spec}(\mathbb{Z})$ 的图像



命题 2.6.1 $\forall z \in \mathbb{Z}[i]$ 均有素分解

证明 即证明 $\forall z \in \mathbb{Z}[i]$ 有不可约分解，若素数 $p \mid N(z) = z\overline{z} \in \mathbb{Z}$

Case 1. 若 $p = 4k+3$，则 p 为 Gauss 素数，$p \mid z$

Case 2. 若 $p = 4k+1$，则 $p = a^2 + b^2 \Longrightarrow (a+bi) \mid z$ 或 $(a-bi) \mid z$

Case 3. 若 $p = 2$，则 $(1+i) \mid z$

对 $\frac{z}{p}$ 或 $\frac{z}{a \pm bi}$ 或 $\frac{z}{1+i}$ 继续进行上述过程，有限步后停止 □

例 2.46 在 $\mathbb{Z}[i]$ 中，分解 $z = 29 - 2i$

解 因为 $N(z) = z\overline{z} = 29^2 + 2^2 = 5 \times 13^2$，所以可能的因子有 $1 \pm 2i, 2 \pm 3i$，逐个尝试可得 $\frac{29-12i}{1+2i} = 5 - 12i$，又因为 $N(5-12i) = 13^2$，所以可能的因子有 $2 \pm 3i$，逐个尝试可得 $\frac{5-12i}{2+3i} = 2 + 3i$，所以 $29 - 2i = (1+2i)(2+3i)^2$

Fact $(a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2$

证明 $|a+bi|^2 |c+di|^2 = |(a+bi)(c+di)|^2$ □

定理 2.6.3（二平方和定理）对 $\forall n \ge 2$，n 可以写为二平方和当且仅当 n 有标准分解

$$n = 2^l p_1^{m_1} \cdots p_t^{m_t}$$

且当 $p_i = 4k+3$ 时，m_i 为偶数

证明 $(\Longleftarrow)$：由定理2.6.1，$4k+1$ 型素数可以写为二平凡和，即 $p_j^2 = a_j^2 + b_j^2$，所以

$$n = (1^2+1^2)^l \prod_{p_i = 4k+3} (p_i^2 + 0^2)^{\frac{m_i}{2}} \prod_{p_j = 4k+1} (a_j^2 + b_j^2)^{m_j}$$

再结合上面的 Fact，即可将 n 表示为二平方和（表达不唯一!）

$(\Longrightarrow)$：若 $n = a^2 + b^2 = (a+bi)(a-bi)$，将 $z = a+bi$ 在 $\mathbb{Z}[i]$ 中进行素分解得 $z = z_1 \cdots z_n$，不难看出 $n = N(z_1) \cdots N(z_n)$ 即为标准分解 □

Ex P92 T2

Ex 设 $a, b \in \mathbb{Z}, \gcd(a,b) = 1$，求证 $\mathbb{Z}[i]/(a^2+b^2) \simeq \mathbb{Z}/(a^2+b^2)$

§2.7 唯一分解整环

定义 2.7.1（唯一分解整环）整环 R 称为唯一分解整环 UFD(unique factorization domain)，若对 $\forall a \in R$

(1) 存在不可约分解：$\exists c_1, \cdots, c_r \in R$ 不可约，使得 $a = c_1 \cdots c_r$

(2) 不可约分解唯一：若 $\exists c_1, \cdots, c_r, d_1, \cdots, d_s$ 不可约，使得 $a = c_1 \cdots c_r = d_1 \cdots d_s$，则 $r = s$，且在调整顺序后，c_i 和 d_i 相伴

Fact 设 R 为 UFD，则

(1) 不可约元与素元等价

Proof : 只需证明不可以元是素元，假设 $a \in R$ 不可约，且非零非单位，若 $a \mid bc$，则 $\exists d \in R, \text{s.t. } ad = bc$，对 b, c, d 作不可约分解得

$$ad_1 \cdots d_r = (b_1 \cdots b_s)(c_1 \cdots c_t)$$

由不可约分解唯一知，存在某个 b_i 或 c_i 使得 a 与其相伴，因此 $a \mid b$ 或 $a \mid c$

(2) R 中有标准分解，即 $\forall a \in R, \exists u \in U(R), p_i$ 为素元且互不相伴，使得

$$a = up_1^{n_1} \cdots p_r^{n_r}$$

则在相伴意义下，a 的因子总形如

$$vp_1^{m_1} \cdots p_r^{m_r}, \quad \forall i, 0 \le m_i \le n_i, v \in U(R)$$

(3) 对 $\forall a, b \in R, \gcd(a, b), \operatorname{lcm}(a, b)$ 存在：设 $a = up_1^{n_1} \cdots p_r^{n_r}, b = vp_1^{m_1} \cdots p_r^{m_r}$，其中 $\forall i, n_i, m_i \ge 0, u, v \in U(R)$，则

$$\gcd(a, b) \overset{\text{相伴}}{\sim} \prod_{i=1}^{r} p_i^{\min\{n_i, m_i\}}, \quad \operatorname{lcm}(a, b) \overset{\text{相伴}}{\sim} \prod_{i=1}^{r} p_i^{\max\{n_i, m_i\}}$$

(4) $K \overset{\text{def}}{=} \operatorname{Frac}(R)$ 中有即约表达，即 $\forall a, b \in \operatorname{Frac}(R), \exists a', b' \in R, \text{s.t. } \frac{a}{b} = \frac{a'}{b'}$，其中 $\gcd(a', b') = 1$，且即约表达 $\frac{a'}{b'}$ 在相伴意义下唯一，即若 $\frac{a'}{b'} = \frac{a''}{b''}$，则 $a' \overset{\text{相伴}}{\sim} a'', b' \overset{\text{相伴}}{\sim} b''$

评价 在 UFD 中，不可约分解与素分解是一回事

定义 2.7.2（生成理想）设 $X \subseteq R$ 是环 R 的子集，称

$$(X) = RX = \left\{ \text{有限和} \sum_{i=1}^{n} a_i x_i | a_i \in R, x_i \in X \right\} \lhd R$$

为由 X 生成的理想，它是包含 X 的最小理想，若 X 是有限集合，则称 $(X) = RX$ 是有限生成理想

评价 特别地，若 $X = \{a\}$，则 $(X) = (a)$ 就是先前定义的主理想

定义 2.7.3（Noether）环 R 称为 Noether 环，若任意理想均有限生成

例 2.47 根据定义知 PID 是 Noether 环

定理 2.7.1（Hilbert 基定理）设 R 是 Noether 环，则 $R[x_1,\cdots,x_n]$ 以及其商环均为 Noether 环

评价 由 $R[x_1,\cdots,x_n]\simeq R[x_1,\cdots,x_{n-1}][x_n]$ 知，只需证明若 R 是 Noether 环，则 $R[x]$ 是 Noether 环；由对应定理2.2.2知 R 的商环的理想也是有限生成的；但是上课没有给出具体证明

定理 2.7.2 设 R 是 Noether 环，则 $\forall a\in R$ 均存在不可约分解

证明 设 $\exists a\in R\backslash U(R)$ 没有不可约分解，若 $a=a_1a_2$，则 a_1,a_2 必有一者没有不可约分解，不妨设为 a_1，若 $a_1=a_{11}a_{12}$，依此类推我们得到严格的理想升链

$$(a)\subsetneqq(a_1)\subsetneqq(a_{11})\subsetneqq\cdots$$

由下面的练习知，这是不可能的 □

Ex 设 R 是 Noether 环，则理想升链 $I_1\subsetneqq I_2\subsetneqq\cdots$ 稳定，即 $\exists N>0,\text{s.t. } I_N=I_{N+1}=\cdots$

Fact 设 R 是整环，若 $a\in R$ 有素分解 $a=p_1\cdots p_r$，则 a 的不可约分解在相伴意义下唯一

证明 设 $a=c_1\cdots c_s$ 为 a 的一个不可约分解，则 $\exists c_i,\text{s.t. } p_1\mid c_i$，不妨设 $p_1\mid c_1$，又因为 c_1 是不可约元，所以 p_1 与 c_1 相伴，继续进行上述过程可知 $r=s$，且 p_i 与 c_i 相伴 □

推论 2.7.1 设 R 是整环，则 R 是 UFD $\iff$ $\forall a\in R$ 存在素分解

推论 2.7.2 设整环 R 中每个非零非单位元素都有不可约分解，则 R 是 UFD $\iff$ R 中素元与不可约元等价

评价 PID 是 Noether 环；ED 是 PID 是 UFD

定理 2.7.3（Gauss 定理）若 R 是 UFD，则 $R[x]$ 是 UFD

例 2.48 $\mathbb{Z}[x]$ 是 UFD 但不是 PID，考虑 $(2,x)$，它不能被一个元素表示；$k[x,y]$ 是 UFD，但不是 PID

为了证明高斯定理，我们需要一些铺垫

定义 2.7.4（容度）设 $f(x)=a_nx^n+\cdots+a_1x+a_0\in R[x],a_n\neq 0_R$，定义 $f(x)$ 的容度为 $c(f)=\gcd(a_0,\cdots,a_n)\in R$

定义 2.7.5（本原多项式）称 $f(x)\in R[x]$ 是本原多项式，若 $c(f)\overset{相伴}{\sim}1_R$，实际上我们可以对 $\forall f(x)\in R[x]$ 进行本原化，即 $f(x)=c(f)f_0(x)$，其中 $f_0(x)$ 为本原多项式

引理 2.7.1（Gauss 引理）设 $f(x),g(x)\in R[x]$ 为本原多项式，则 $f(x)g(x)\in R[x]$ 也是本原多项式

证明 设 $f(x)=a_nx^n+\cdots+a_1x+a_0, g(x)=b_mx^m+\cdots+b_1x+b_0$ 是本原多项式，下证 $f(x)g(x)$ 本原

方法一：因为 $f(x)g(x)=\sum\limits_{l=0}^{m+n}c_lx^l, c_l=\sum\limits_{i+j=l}a_ib_j, 0\le l\le m+n$，我们断言：$\gcd(c_0,\cdots,c_{m+n})=1$

Proof Of Claim：否则，$\exists p\in R$ 素元，使得 $p\mid c_0,\cdots,p\mid c_{m+n}$，又因为

$$\begin{cases}\exists!0\le i_0\le n,\text{s.t. } p\mid a_0,\cdots p\mid a_{i_0-1},\text{但}p\nmid a_{i_0}\\ \exists!0\le j_0\le m,\text{s.t. } p\mid b_0,\cdots p\mid b_{j_0-1},\text{但}p\nmid b_{j_0}\end{cases}$$

考虑 $c_{i_0+j_0}=(a_0b_{i_0+j_0}+\cdots+a_{i_0-1}b_{j_0+1})+a_{i_0}b_{j_0}+(a_{i_0+1}b_{j_0-1}+\cdots+a_{i_0+j_0}b_0)$，由 $p\mid c_{i_0+j_0}$ 知，$p\mid a_{i_0}b_{j_0}$，故 $p\mid a_{i_0}$ 或 $p\mid b_{j_0}$，但这与假设矛盾 □

方法二：反证假设同上，考虑模 p 约化，我们有满同态

$$\begin{aligned}\pi: R&\longrightarrow\!\!\!\!\!\rightarrow R/(p)\\ r&\longmapsto\overline{r}\end{aligned}$$

它诱导了多项式环同态

$$\begin{aligned}\tilde{\pi}: R[x]&\longrightarrow\!\!\!\!\!\rightarrow \big(R/(p)\big)[x]\\ h(x)&\longmapsto\overline{h(x)}\end{aligned}$$

其中若 $h(x)=a_nx^n+\cdots+a_1x+a_0$，则 $\overline{h(x)}=\overline{a}_nx^n+\cdots+\overline{a}_1x+\overline{a}_0$，由假设知 $\tilde{\pi}(fg)=\overline{0}$，而由 p 是素元知，$R/(p)[x]$ 是整环，因此 $\tilde{\pi}(f)=0$ 或 $\tilde{\pi}(g)=0$，这与 $f(x),g(x)$ 是本原多项式矛盾！ □

Ex 证明：$\forall c\in R, R[x]/(c)\simeq R/(c)[x]$

接下来我们可以证明 Gauss 定理2.7.3

证明 对 $\forall f(x)\in R[x]$，我们可以将 $f(x)$ 本原化，即 $f(x)=c(f)f_0(x)$，其中 $f_0(x)$ 是本原多项式

Step 1. 对容度 $c(f)$ 在 $R[x]$ 中进行分解：因为 R 是 UFD，所以 $c(f)$ 在 R 中有素分解 $c(f)=c_1\cdots c_r$，再由上面的练习知，$R/(c_i)[x]\simeq R[x]/(c_i)$，因为 $c_i\in R$ 是素元，所以 $R/(c_i)[x]$ 是整环，故 $R[x]/(c_i)$ 也是整环，则 $c_i\in R[x]$ 也是素元，所以 $c(f)=c_1\cdots c_r$ 也是 $R[x]$ 中的素分解

Step 2. 记 $K=\mathrm{Frac}(R)$，因为 $K[x]$ 是 ED $\Longrightarrow$ PID $\Longrightarrow$ UFD，所以在 $K[x]$ 中有

$$f_0(x)=f_1(x)\cdots f_s(x),\quad \forall i, f_i(x)\in K[x]\text{不可约}$$

对于任意 $f_i(x)\in K[x]$，我们可以通过通分（乘以分母的公倍数）使得 $f_i(x)=\frac{1}{a_i}\tilde{f}(x)$，其中 $\tilde{f}_i(x)\in R[x]$，再对 $\tilde{f}_i(x)$ 取容度得 $f_i(x)=\frac{c(\tilde{f})}{a_i}\bar{f}_i(x)$，其中 $\bar{f}_i(x)$ 本原，因此我们可以一开始就不妨设 $f_i(x)=\frac{1}{a_i}\tilde{f}(x)$，其中 $\tilde{f}(x)$ 本原（谨慎通分），所以我们有

$$f_0(x)=\frac{1}{a_1\cdots a_s}\tilde{f}_1(x)\cdots\tilde{f}_s(x),\quad \forall i,\tilde{f}_i(x)\text{本原}$$

由 Gauss 引理知，$\frac{1}{a_1\cdots a_s} \overset{相伴}{\sim} 1_R$

Step 3. 证明 $\tilde{f}_i(x)$ 在 $R[x]$ 中是素元，假设 $\tilde{f}_i(x)=u(x)v(x)$ in $R[x]$，则在 $K[x]$ 中也有 $\tilde{f}_i(x)\mid u(x)v(x)$，而 $\tilde{f}_i(x)$ 在 $K[x]$ 中是素元，可不妨设 $\tilde{f}_i(x)\mid u(x)$ in $K[x]$，故 $\exists h(x)\in K[x],\text{s.t. }\tilde{f}_i(x)h(x)=u(x)$，可设 $h(x)=\frac{m}{n}\tilde{h}(x)$，其中 $\tilde{h}(x)$ 本原，则 $nu(x)=m\tilde{f}_i(x)\tilde{h}(x)$，两边同时取容度得 $nc(u)=m$，即 $u(x)=c(u)\tilde{f}_i(x)\tilde{h}(x)$，而 $u(x)\in R\Longrightarrow c(u)\in R$，所以 $\tilde{f}_i(x)\mid u(x)$ in $R[x]$，所以 $\tilde{f}_i(x)$ 在 $R[x]$ 中是素元

综上 $f(x)=uc_1\cdots c_r\tilde{f}_1(x)\cdots\tilde{f}_s(x)$ 为 $f(x)$ 的素分解，再由推论2.7.1即得证 □

命题 2.7.1 设 R 是 UFD, $K=\mathrm{Frac}(R)$，若 $f(x)\in R[x]$ 本原，则

$$f(x)在R[x]中不可约 \iff f(x)在K[x]中不可约$$

Ex 证明留作练习

例 2.49 求证 $f(x)=x^3+3x-2$ 在 $\mathbb{Q}[x]$ 中不可约

证明 由命题2.7.1,只需证明 $f(x)$ 在 $\mathbb{Z}[x]$ 上不可约,假设 $f(x)$ 可约,则一定存在因子 $(3=1+2=1+1+1)$，故 $f(x)$ 有整数根 $x=a$，可设 $f(x)=(x-a)(x^2+bx+c)$，因此 $ac=2$，即 $a\mid 2, a=\pm1,\pm2$，但是经过计算 $f(\pm1), f(\pm2)\neq 0$，矛盾！ □

命题 2.7.2（Eisenstein 判别法）设 R 是 UFD, $f(x)=c_nx^n+\cdots+c_1x+c_0\in R[x]$ 是本原多项式，若 $\exists p\in R$ 素元，满足

(1) $p\nmid c_n$

(2) $p\mid c_{n-1},\cdots,p\mid c_1, p\mid c_0$

(3) $p^2\nmid c_0$

则 $f(x)\in R[x]$ 不可约，进而 $f(x)\in K[x]$ 不可约

评价 实际上条件 (2) 加上 f 本原可以推出条件 (1)

证明 方法一:设 $f(x)=g(x)h(x), g(x)=\sum\limits_{i=0}^{r}a_ix^i, h(x)=\sum\limits_{j=0}^{n-r}b_jx^j$,则 $g(x),h(x)$ 本原,$p\mid c_0=a_0b_0, p^2\nmid c_0$，因此不妨设 $p\mid a_0$ 但 $p\nmid b_0$，则 $\exists!1\le i_0\le r-1,\text{s.t. }p\mid a_0,\cdots,p\mid a_{i_0-1}$，但 $p\nmid a_{i_0}$（若 $i_0=r$，则将导致 $p\mid c_n$，矛盾!），则

$$c_{i_0}=a_{i_0}b_0+a_{i_0-1}b_1+\cdots+a_0b_{i_0}$$

由 $p\mid c_{i_0}$ 知，$p\mid a_{i_0}b_0$，这与 $p\nmid a_{i_0}, p\nmid b_0$ 矛盾！

方法二：模 p 约化，考虑满同态

$$\begin{aligned}\pi: R[x]&\longrightarrow R/(p)[x]\\ x&\longmapsto x\\ a&\longmapsto \overline{a}\end{aligned}$$

则 $\overline{c}_nx^n=\pi(f)=\pi(g)\pi(h)$，故 $\pi(g),\pi(h)$ 的常数项系数均为 $\overline{0}$，故 $p^2\mid c_0$，矛盾！ □

例 2.50 $\forall n \geq 1, x^2-2 \in \mathbb{Q}[x]$ 不可约

证明 即证明 $x^2-2 \in \mathbb{Z}[x]$ 不可约，取素数 $p=2$，由 Eisenstein 判别法即证 □

Ex 设 $g(x)=a_nx^n+\cdots+a_1x+a_0 \in \mathbb{Z}[x]$，定义 $g(x+b)=a_n(x+b)^n+\cdots+a_1(x+b)+a_0$，证明
(1) $g(x)$ 本原 $\iff$ $g(x+b)$ 本原
(2) $g(x)$ 不可约 $\iff$ $g(x+b)$ 不可约

评价 将 $\mathbb{Z}$ 换为一般的 UFD 均对

例 2.51 设 p 是素数，则 $f(x)=1+x+\cdots+x^{p-1}=\frac{x^p-1}{x-1} \in \mathbb{Q}[x]$ 不可约

证明 由上面的练习，只需证明 $f(x+1)$ 在 $\mathbb{Z}[x]$ 中不可约即可，因为

$$f(x+1)=\frac{(x+1)^p-1}{x}=\sum_{i=0}^{p-1}\binom{p}{i+1}x^i$$

取素数 p，由 Eisenstein 判别法知 $f(x+1)$ 不可约

例 2.52 $f(x,y)=y^3-x^2 \in k[x,y]=\big(k[x]\big)[y]$ 不可约

证明 假设它可约，将它视为以 $k[x]$ 中元素为系数，以 y 为字母的多项式，则 $k[x][y]$ 中有分解

$$y^3-x^2=[y-a(x)]\cdot[y^2+b(x)y+c(x)]$$

所以 $m(x)^3-x^2=0$，这显然无解，故矛盾！ □

评价 由于 $y^3-x^2 \in k[x,y]$ 不可约，且它是 $k[x,y]=k[x][y]$ 中的本原多项式，又因为 $k(x)=\mathrm{Frac}(k[x])$，故 y^3-x^2 在 $k(x)[y]$ 中不可约，则 $k(x)[y]/(y^3-x^2)$ 是域，且 $k(x)[y]/(y^3-x^2) \simeq \mathrm{Frac}\,(k[x,y]/(y^3-x^2))$

Ex 设 $R=k[t], t$ 是字母，令 $S=\{f(t) \in R | f(t)$的t^1项系数为零$\}$，求证
(1) $S \simeq k[x,y]/(y^3-x^2)$
(2) $\mathrm{Frac}(S)=k(t)$

评价 S 是 R 的子环，但是 S 不是 UFD，因为 $t^6=t^3\cdot t^3=t^2\cdot t^2\cdot t^2$

§2.8 中国剩余定理

定义 2.8.1（环的直积）设 $R_1,\cdots,R_s$ 均为环，在 $R_1\times\cdots\times R_s$ 中定义加法与乘法如下

$$\begin{cases}(a_1,\cdots,a_s)+(b_1,\cdots,b_s)=(a_1+b_1,\cdots,a_s+b_s)\\(a_1,\cdots,a_s)\cdot(b_1,\cdots,b_s)=(a_1b_1,\cdots,a_sb_s)\end{cases}$$

容易验证 $(R_1\times\cdots\times R_s,+,\cdot)$ 是一个环，称为 $R_1,\cdots,R_s$ 的直积，它的零元是 $(0_{R_1},\cdots,0_{R_s})$，幺元是 $(1_{R_1},\cdots,1_{R_s})$

评价 $R_1\times\cdots\times R_s$ 不是整环，比如 $(0,1,\cdots,1)\cdot(1,0,\cdots,0)=(0,\cdots,0)$

Fact $U(R\times S)=U(R)\times U(S)$

定义 2.8.2（互素）若 $I\lhd R, J\lhd R$，且 $I+J=R$，则称 I 与 J 互素

命题 2.8.1 设 $\{I_i\}_{i=1}^n$ 是 R 的一族理想，且 $\forall i\neq j, I_i$ 与 I_j 互素，则

$$I_i+\prod_{j\neq i} I_i=R, \forall i$$

证明 由对称性只需证明 $I_1+I_2\cdots I_n=R$，因为 $IJ\subset I$，所以

$$\begin{aligned} R=RR&=(I_1+I_2)(I_1+I_3)\\ &=I_1(I_1+I_2+I_3)+I_2I_3\\ &\subset I_1+I_2I_3\subset R \end{aligned}$$

即 $R=I_1+I_2I_3$，假设命题对 $n-1$ 成立，则

$$R=RR=(I_1+I_n)(I_1+I_2\cdots I_{n-1})=I_1(I_1+I_n+I_2\cdots I_{n-1})+I_n\subset I_1+I_n\subset R$$

即 $R=I_1+I_2\cdots I_n$ □

命题 2.8.2 设 $I\lhd R, J\lhd R, I+J=R$，则 $I\cap J=IJ$

证明 一方面，因为 $IJ\subset I, IJ\subset J$，所以 $IJ\subset I\cap J$；另一方面，因为 $I+J=R$，所以 $\exists u\in I, v\in J, \text{s.t. } u+v=1$，则 $\forall x\in I\cap J, x=ux+vx\in IJ$，即 $IJ\subset I\cap J$，综上有 $IJ=I\cap J$ □

评价 由数学归纳法，该命题可推广到一般情形，即 $I_1\cap\cdots\cap I_n=I_1\cdots I_n$

定理 2.8.1（中国剩余定理）设 R 是环，$I_1,\cdots,I_n\lhd R$，若 $\forall i\neq j, I_i+I_j=R$，即它们两两互素，则环同态

$$\begin{aligned} \phi: R&\longrightarrow (R/I_i)\times\cdots\times(R/I_n)\\ r&\longmapsto (r+I_1,\cdots,r+I_n) \end{aligned}$$

是满同态，且它诱导了环同构

$$\tilde{\phi}: R/(I_1\cdots I_n)\xrightarrow{\sim}(R/I_i)\times\cdots\times(R/I_n)$$

证明 先证 ϕ 是满射：即对 $\forall(a_1+I_1,\cdots,a_n+I_n)\in\prod_{i=1}^n(R/I_i)$，要找到 $b\in R, \text{s.t. } \phi(b)=(a_1+I_1,\cdots,a_n+I_n)$，即同余方程组

$$\begin{cases} b\equiv a_1 \mod I_1\\ \cdots\cdots\\ b\equiv a_n \mod I_n \end{cases}$$

有解 $b \in R$，由命题2.8.1知，$I_1 + I_2 \cdots I_n \in R \Longrightarrow \exists \xi_1 \in I_1, b_1 \in I_2 \cdots I_n, \text{s.t. } \xi_1 + b_1 = 1$，则

$$\begin{cases} b_1 \equiv 1 & \mod I_1 \\ b_1 \equiv 0 & \mod I_2 \\ \quad \cdots\cdots\cdots & \\ b_1 \equiv 0 & \mod I_n \end{cases}$$

类似可以找到 $b_i, \forall i$，取 $b = a_1 b_1 + \cdots + a_n b_n$ 即为所求，故 ϕ 是满射

再证 $\text{Ker}(\phi) = I_1 \cap \cdots \cap I_n$，这是因为

$$\begin{aligned} a \in \text{Ker}(\phi) &\iff a \equiv 0 \mod I_i, \forall i \iff a \in I_i, \forall i \\ &\iff a \in I_1 \cap \cdots \cap I_n \end{aligned}$$

所以 $\text{Ker}(\phi) = I_1 \cap \cdots \cap I_n$，进而由环同态基本定理2.2.1知有环同构

$$R/(I_1 \cap \cdots \cap I_n) \xrightarrow{\sim} (R/I_i) \times \cdots \times (R/I_n)$$

最后结合命题2.8.2知，$I_1 \cdots I_n = I_1 \cap \cdots \cap I_n$，故有环同构

$$\tilde{\phi} : R/(I_1 \cdots I_n) \xrightarrow{\sim} (R/I_i) \times \cdots \times (R/I_n)$$

□

例 2.53 设 $m, n \in \mathbb{Z}, \gcd(m, n) = 1$，则

$$\mathbb{Z}_{mn} = \mathbb{Z}/(mn) = \frac{\mathbb{Z}}{(m) \cap (n)} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$$

第三章 域

§3.1 基本定义与单扩张

定义 3.1.1（域扩张）域扩张是指域同态 $\theta : k \hookrightarrow K$，记作 K/k

评价 (1) 有域同构

$$\begin{aligned} \theta : k &\xrightarrow{\sim} \theta(k) \overset{\text{子域}}{\subseteq} K \\ \lambda &\longmapsto \theta(\lambda) \in K \end{aligned}$$

即我们可以将 k 与 K 的子域 $\theta(k)$ 等同起来，但是记号 K/k 真事隐，它没有体现 θ 的信息

(2) 给定 $\theta : k \hookrightarrow K, K$ 自然成为 k-线性空间，加法数乘定义为

- 加法：$\forall \boldsymbol{v}_1, \boldsymbol{v}_2 \in K, \boldsymbol{v}_1 + \boldsymbol{v}_2 \in K$
- 数乘：$\forall \boldsymbol{v} \in K, \lambda \in k, \lambda \cdot \boldsymbol{v} = \theta(\lambda) \cdot \boldsymbol{v}$

例 3.1 $\mathrm{Id}_{\mathbb{C}} : \mathbb{C} \to \mathbb{C}, \sigma : \mathbb{C} \to \mathbb{C}, z \mapsto \overline{z}$ 都记为 $\mathbb{C}/\mathbb{C}$，但实际上它们表示的是不同的域扩张，故记号 K/k 是“危险”的记号

定义 3.1.2（域扩张的维数）称 K 作为 k-线性空间的维数为域扩张 K/k 的维数，记作 $\dim_k K$ 或 $[K : k]$

例 3.2（添根构造）设 $f(x) \in k[x]$ 首一不可约，$\deg(f(x)) \geq 2$，则 $(f(x)) \in \mathrm{Max}(k[x])$，因此 $K = k[x]/(f(x))$ 是域，我们有域扩张

$$\begin{aligned} k &\hookrightarrow K \\ \lambda &\longmapsto \overline{\lambda}, \text{仍记为} \lambda \end{aligned}$$

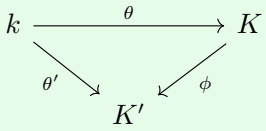
由先前分析知，$\dim_k K = \deg(f(x)) \overset{\text{记为}}{=} d$，记 $u = \overline{x} \in K$，则 $u \in \mathrm{Root}_K(f)$，且 K 有一组 k-基 $\{1, u, \cdots, u^{d-1}\}$

例 3.3 设 k 为域，$k(x) = \mathrm{Frac}(k[x]) = \left\{ \dfrac{f(x)}{g(x)} \middle| f(x), g(x) \in k[x], g(x) \neq 0 \right\}$，由 $k[x]$ 是 UFD 知，$\dfrac{f(x)}{g(x)} \in k(x)$ 有即约表达，我们有域扩张

$$\begin{aligned} k &\hookrightarrow k(x) \\ \lambda &\longmapsto \frac{\lambda}{1}, \text{仍记为} \lambda \end{aligned}$$

Fact $\dim_k K = +\infty$，因为 $\left\{ \frac{1}{1}, \frac{x}{1}, \frac{x^2}{1}, \cdots \right\}$ 是 k-线性无关的

定义 3.1.3（域扩张的同构）设 $\theta : k \hookrightarrow K, \theta' : k \hookrightarrow K'$，称 θ, θ' 是域扩张的同构，若存在域同构 $\phi : K \xrightarrow{\sim} K', \text{s.t. } \phi \circ \theta = \theta'$，即下面的图交换



评价 ϕ 是 k-线性同构，故保域扩张的维数，即 $\dim_k K = \dim_k K'$

Ex 设 $K = k(t), m, n \geq 2$ 且 $m \neq n$，考虑域扩张

$$\begin{aligned} \theta_1 : K &\hookrightarrow K & \theta_2 : K &\hookrightarrow K \\ \frac{f(t)}{g(t)} &\longmapsto \frac{f(t^m)}{f(t^m)} & \frac{f(t)}{g(t)} &\longmapsto \frac{f(t^n)}{f(t^n)} \end{aligned}$$

求证 θ_1, θ_2 不同构

定义 3.1.4（域扩张的自同构）域扩张 $\theta : k \hookrightarrow K$ 的自同构是指域同构 $\varphi : K \xrightarrow{\sim} K$，满足 $\varphi \circ \theta = \theta$，我们称 $\mathrm{Aut}(K/k) = \{\varphi \in \mathrm{Aut}(K) | \varphi \circ \theta = \theta\}$ 记为域扩张 K/k 的自同构群

评价 称 $\mathrm{Aut}(K)$ 为 K 的自同构群，则 $\mathrm{Aut}(K/k) \leq \mathrm{Aut}(K)$；我们定义的 $\mathrm{Aut}(K/k)$ 实际上隐藏了 θ 的信息，但是实际上大部分 $\mathrm{Aut}(K/k)$ 中的 θ 都是 Id_k，即大部分语境下有

$$\mathrm{Aut}(K/k) = \{\varphi \in \mathrm{Aut}(K) : \varphi|_k = \mathrm{Id}_k\}$$

接下来进行一些符号约定

定义 3.1.5 设 $R \overset{\text{子环}}{\subseteq} S, \alpha \in S$，定义

$$R[\alpha] \overset{\text{def}}{=} \left\{ \sum_{i=0}^{n} r_i \alpha^i \middle| r_i \in R \right\}$$

为包含 R 及 α 的最小子环；若为环嵌入 $\theta : R \hookrightarrow S, \alpha \in S$，我们类似定义

$$R[\alpha] \overset{\text{def}}{=} \theta(R)[\alpha] = \left\{ \sum_{i=0}^{n} \theta(r_i) \alpha^i \middle| r_i \in R \right\}$$

为包含 $\theta(R)$ 及 α 的最小子环

评价 (1) 上述求和要求为有限和，约定 $\alpha^0 = 1_R$

(2) 若为 $R \overset{\text{子环}}{\subseteq} S$，则我们有满同态

$$\begin{aligned} R[x] &\twoheadrightarrow R[\alpha] \\ f(x) &\longmapsto f(\alpha) \end{aligned}$$

若为 $R \hookrightarrow S$，则我们有满同态

$$\begin{aligned} R[x] &\longrightarrow R[\alpha] \\ f(x) &\longmapsto \theta(f)(\alpha) \end{aligned}$$

(3) 类似地，我们可以定义 $R[\alpha_1, \alpha_2] = R[\alpha_1][\alpha_2] = R[\alpha_2][\alpha_1]$

定义 3.1.6 设 $k \overset{\text{子域}}{\subseteq} K, \alpha \in K$，定义

$$k(\alpha) \overset{\text{def}}{=} \left\{ \frac{\sum_{i=0}^{n} r_i \alpha^i}{\sum_{j=0}^{m} r_j \alpha^j} \middle| r_i, r_j \in k, \sum_{j=0}^{m} r_j \alpha^j \neq 0_K \right\}$$

为包含 k 和 α 的最小子域；若为域嵌入 $\theta : k \hookrightarrow K$，我们类似定义

$$k(\alpha) \overset{\text{def}}{=} \left\{ \frac{\sum_{i=0}^{n} \theta(r_i) \alpha^i}{\sum_{j=0}^{m} \theta(r_j) \alpha^j} \middle| r_i, r_j \in k, \sum_{j=0}^{m} \theta(r_j) \alpha^j \neq 0_K \right\}$$

为包含 $\theta(k)$ 和 α 的最小子域

评价 (1) $k[\alpha] \subseteq k(\alpha)$
(2) $k(\alpha)$ 与 $k[x]$ 可能不相关

例 3.4 $\mathbb{Q} \subseteq \mathbb{C}$，则 $\mathbb{Q}(i) = \mathbb{Q}[i] = \{a + bi | a, b \in \mathbb{Q}\}$

定义 3.1.7（单扩张）域扩张 K/k 称为单扩张，若 $\exists \alpha \in K, \text{s.t. } K = k(\alpha)$，我们称 α 为域扩张 K/k 的生成元

例 3.5 添根构造 $k \hookrightarrow K = k[x]/(f(x))$ 是单扩张，因为 $K = k(u) = k[u]$

例 3.6 $k \hookrightarrow k(x)$ 是单扩张，生成元为 x，但是 $k[x] \subsetneq k(x)$

例 3.7 $\mathbb{Q} \subseteq \mathbb{Q}(i)$ 是单扩张；$\mathbb{Q} \subseteq \mathbb{C}$ 也是单扩张，因为 $\mathbb{C} = \mathbb{R}(i) = \mathbb{R}[i]$

定义 3.1.8（代数、超越元）设有域扩张 K/k，称 $\alpha \in K$ 为 k 上代数元，若存在非零多项式 $f(x) \in k[x], \text{s.t. } f(\alpha) = 0$，即若 $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$，则

$$f(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1 \alpha + a_0 = 0$$

否则，则称 $\alpha \in K$ 是 k 上的超越元

评价 $\forall a \in k, \alpha = \theta(a) \in K$ 一定是 k 上的代数元，只需取 $f(x) = x - \alpha$ 即可

例 3.8 考虑域扩张 $\mathbb{C}/\mathbb{Q}, \sqrt{2} \in \mathbb{C}$ 为 $\mathbb{Q}$ 上代数元，因为 $f(x) = x^2 - 2, f(\sqrt{2}) = 0$；由数学分析的知识知，$\pi, e$ 不是 $\mathbb{Q}$ 上的代数元

例 3.9 考虑添根构造 $k \hookrightarrow K = k[x]/(f(x))$，由 $f(u) = 0_K$ 知，u 是 k 上代数元，我们断言：$\forall 0 \neq z \in K$ 均为 k 上代数元，因为 $\dim_k K = \deg(f) \overset{\text{def}}{=} d$，则

$$\{1, z, \cdots, z^{d-1}\} \ k\text{-线性相关}$$

即 $\exists \lambda_0, \cdots, \lambda_{d-1} \in k, \text{s.t. } \lambda_0 + \lambda_1 z + \cdots + \lambda_{d-1} z^{d-1} = 0$，取 $f(x) = \lambda_0 + \lambda_1 x + \cdots + \lambda_{d-1} x^{d-1}$，则 $f(z) = 0$

Ex 考虑 $k \hookrightarrow k(t), t$ 是 k 上的超越元，求证：$\forall \frac{f(t)}{g(t)} \in k(t)\backslash k$ 均为 k 上的超越元

定理 3.1.1（最小多项式）设有域扩张 $K/k, \alpha \in K$ 是 k 上的代数元，则存在唯一首一不可约多项式 $f(x) \in k[x]$ 满足 $f(\alpha) = 0_K$，我们称 $f(x)$ 为 α 在 k 上的最小多项式

证明 考虑赋值同态

$$\begin{aligned} \mathrm{ev}_\alpha : k[x] &\longrightarrow K \\ g(x) &\longmapsto g(\alpha) \end{aligned}$$

由于 $k[x]$ 是 PID，所以 $\exists f(x) \in k[x], \text{s.t. } \mathrm{Ker}(\mathrm{ev}_\alpha) = (f(x))$，由环同态基本定理知，存在环同构

$$k[x]/(f(x)) \simeq \mathrm{Im}(\mathrm{ev}_\alpha) = k[\alpha]$$

因为 $k[\alpha] \subseteq K$ 为整环，所以 $k[x]/(f(x))$ 也为整环，故 $f(x)$ 是 $k[x]$ 上的素元，即 $f(x)$ 是 $k[x]$ 上的不可约多项式，由 f 首一保证唯一性 □

评价 (1) 一般我们默认 $k \subseteq K$ 是子域，即 $\theta = \mathrm{inc}$，若为 $\theta : k \hookrightarrow K$，则 $f(\alpha) = 0_K$ 实际上是 $\theta(f)(\alpha) = 0_K$

(2) 讨论最小多项式时，一定要说明是哪个域上的最小多项式，见下面例3.11

(3) 对 $\forall g(x) \in k[x]$，若 $g(\alpha) = 0$，则 $g(x) \in \mathrm{Ker}(\mathrm{ev}_\alpha) \Longrightarrow f(x) \mid g(x)$，即 α 的零化多项式一定被 f 整除

(4) 由于 $k[x]/(f(x)) \simeq k[\alpha]$，且 $k[x]/(f(x))$ 是域，故 $k[\alpha]$ 也是域，此时有 $k(\alpha) = \mathrm{Frac}(k[\alpha]) = k[\alpha]$，即对于代数扩张，$k[\alpha] = k(\alpha)$

例 3.10 考虑域扩张 $\mathbb{C}/\mathbb{Q}$，则

- $\sqrt{2}$ 在 $\mathbb{Q}[x]$ 上的最小多项式为 $x^2 - 2$
- $\sqrt{3}$ 在 $\mathbb{Q}[x]$ 上的最小多项式为 $x^2 - 3$
- $\omega = e^{\frac{2\pi i}{3}}$ 在 $\mathbb{Q}[x]$ 上的最小多项式为 $x^2 + x + 1$

例 3.11 考虑域扩张 $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ 和 $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$，则 $\sqrt[4]{2}$ 在 $\mathbb{Q}$ 上的最小多项式为 $x^4 - 2$（取 $p = 2$ 用 Eisenstein 判别法），但 $\sqrt[4]{2}$ 在 $\mathbb{Q}(\sqrt{2})$ 上的最小多项式为 $x^2 - \sqrt{2}$

Ex 求 $\sqrt{2} + \sqrt{3}, \sqrt{3} + \omega$ 在 $\mathbb{Q}$ 上的最小多项式

评价 一般做法是求得一个零化多项式，再观察它是否有因式或是否可约，例如求 $\sqrt{2} + \sqrt{3}$ 在 $\mathbb{Q}$ 上的最小式，设 $\alpha = \sqrt{2} + \sqrt{3}$，则 $\alpha - \sqrt{2} = \sqrt{3}$，两边同时平方得

$$\alpha^2 + 2 - 2\sqrt{2}\alpha = 3 \Longrightarrow \alpha^2 - 1 = 2\sqrt{2}\alpha$$

两边再平方，移项即可得到 $\sqrt{2} + \sqrt{3}$ 的一个零化多项式

定理 3.1.2（单扩张结构定理）设有域扩张 K/k 和 $\alpha \in K, \text{s.t. } K = k(\alpha)$，则

(1) 若 α 是 k 上的代数元，α 在 k 上的最小多项式为 $f(x), \deg(f(x)) = d \geq 1$，则

- $\dim_k K = d < +\infty$

- K 有一组 k-基 $\{1,\alpha,\cdots,\alpha^{d-1}\}$，且 $K=k(\alpha)=k[\alpha]$
- 域扩张 $k\hookrightarrow k(\alpha)=K$ 与域扩张 $k\hookrightarrow k[x]/(f(x))$ 同构

(2) 若 α 是 k 上的超越元，则

- $\dim_k K=+\infty$
- $k[\alpha]\subsetneqq K$
- 域扩张 $k\hookrightarrow k(\alpha)=K$ 与域扩张 $k\hookrightarrow k(x)$ 同构

证明 (1) 考虑赋值同态

$$\begin{aligned}\mathrm{ev}_\alpha : k[x] &\longrightarrow K\\ g(x) &\longmapsto g(\alpha)\end{aligned}$$

同定理3.1.1的证明过程我们有 $\mathrm{Ker}(\mathrm{ev}_\alpha)=(f(x))$，且由 $K=k(\alpha)$ 知 ev_α 是满同态，由环同态基本定理知

$$\begin{aligned}\overline{\mathrm{ev}}_\alpha : k[x]/(f(x)) &\longrightarrow K=k(\alpha)\\ u=\overline{x} &\longmapsto \alpha\end{aligned}$$

是同构，用交换图表示为

$$\begin{array}{ccc} k[x]/(f(x)) & \xrightarrow{\overline{\mathrm{ev}}_\alpha} & K=k(\alpha) \\ & \nwarrow \quad \nearrow & \\ & k & \end{array}$$

(2) 考虑赋值同态

$$\begin{aligned}\mathrm{ev}_\alpha : k[x] &\longrightarrow K=k(\alpha)\\ g(x) &\longmapsto g(\alpha)\end{aligned}$$

由分式域的泛性质2.3.1，存在唯一的域同态 $\tilde{\phi}:\mathrm{Frac}(k[x])=k(x)\hookrightarrow K=k(\alpha)$，满足 $\tilde{\phi}\circ\mathrm{can}_R=\phi$，即下面的图交换

$$\begin{array}{ccc} k[x] & \xrightarrow{\quad\phi\quad} & K=k(\alpha) \\ & {\scriptstyle\mathrm{can}}\searrow \quad \nearrow{\scriptstyle\tilde{\phi}} & \\ & \mathrm{Frac}(k[x])=k(x) & \end{array}$$

显然有 $\tilde{\phi}$ 是满射，且它是域扩张的同构

□

评价 本质上只有以上两种单扩张

Ex 考虑域扩张 $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$，证明

(1) $\mathbb{Q}(\sqrt[3]{2})$ 有一组 $\mathbb{Q}$-基 $\{1,\sqrt[3]{2},\sqrt[3]{4}\}$

(2) 记 $\omega=e^{\frac{2\pi i}{3}}$，证明存在域扩张的同构 $\mathbb{Q}(\sqrt[3]{2}\omega)/\mathbb{Q}\simeq\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$，但是作为集合，$\mathbb{Q}(\sqrt[3]{2}\omega)\neq\mathbb{Q}(\sqrt[3]{2})$

§3.2 代数扩张

定义 3.2.1（代数扩张）域扩张 K/k 称为代数扩张，若 $\forall \alpha \in K, \alpha$ 是 K 上的代数元

引理 3.2.1（有限维域扩张总是代数扩张）设有域扩张 K/k，若 $\dim_k K < +\infty$，则 K/k 是代数扩张

证明 对 $\forall \alpha \in K$，有域扩张塔 $k \subseteq k(\alpha) \subseteq K$，故 $k(\alpha)$ 是 K 的线性子空间，则 $d \overset{\text{def}}{=} \dim_k k(\alpha) \leq \dim_k K < +\infty$，故 $\{1, \alpha, \cdots, \alpha^d\}$ 是 k-线性相关的，因此 α 在 k 上代数 □

定理 3.2.1（维数公式）设有域扩张塔 $k \subseteq E \subseteq K$，若 $E/k, K/E$ 均为有限维域扩张，则 K/k 也是有限维域扩张，且

$$\dim_k K = \dim_k E \cdot \dim_E K$$

证明 设 $\dim_k E = n, \dim_E K = m$,设 E/k 的一组 k-基为 $\{u_1, \cdots, u_n\}, K/E$ 的一组 E-基为 $\{v_1, \cdots, v_m\}$

***Claim*:** K 有一组 k-基 $\{u_i v_j | 1 \leq i \leq n, 1 \leq j \leq m\}$ □

Ex 补全上面的证明

例 3.12 求 $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}, \sqrt{3})$

解 考虑域扩张塔 $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3})$，则

(1) $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2})$: $\sqrt{2}$ 在 $\mathbb{Q}$ 上的最小多项式为 x^2-2，因为 $\sqrt{2} \neq \mathbb{Q}$，所以 $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}) = \deg(x^2-2) = 2$，且 $\mathbb{Q}(\sqrt{2})$ 有一组 $\mathbb{Q}$-基 $\{1, \sqrt{2}\}$

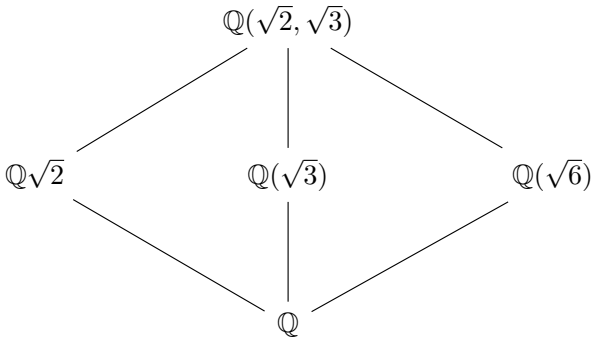
(2) $\dim_{\mathbb{Q}(\sqrt{2})} \mathbb{Q}(\sqrt{2}, \sqrt{3})$: 显然，$x^2-3$ 在 $\mathbb{Q}$ 上的一个零化多项式为 x^2-3，下证它不可约，即证明 $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$，由于 $\mathbb{Q}(\sqrt{2})$ 有一组 $\mathbb{Q}$-基 $\{1, \sqrt{2}\}$，假设 $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$，则 $\exists a, b \in \mathbb{Q}, \text{s.t. } \sqrt{3} = a + b\sqrt{2}$，两边平方得

$$3 = a^2 + 2b^2 + 2\sqrt{2}ab \Longrightarrow \begin{cases} 3 = a^2 + 2b^2 \\ ab = 0 \end{cases}$$

但是上述方程无解，矛盾！所以 $\dim_{\mathbb{Q}(\sqrt{2})} \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \deg(x^2-3) = 2$，且 $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ 有一组 $\mathbb{Q}(\sqrt{2})$-基 $\{1, \sqrt{3}\}$

(3) 由维数公式知 $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}) \cdot \dim_{\mathbb{Q}(\sqrt{2})} \mathbb{Q}(\sqrt{2}, \sqrt{3}) = 2 \times 2 = 4$，结合维数公式的证明知，$\mathbb{Q}(\sqrt{2}, \sqrt{3})$ 有一组 $\mathbb{Q}$-基 $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$

评价 由 Galois 对应知，$\mathbb{Q}(\sqrt{2}, \sqrt{3})$ 的所有子域如下



因此，只需取 $a\in\mathbb{Q}(\sqrt{2},\sqrt{3})\backslash(\mathbb{Q}(\sqrt{2})\cup\mathbb{Q}(\sqrt{3})\cup\mathbb{Q}(\sqrt{6}))$，则 $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(a)$，即 $\mathbb{Q}(\sqrt{2},\sqrt{3})$ 也是单扩张

因为 $\forall a\in\mathbb{Q}(\sqrt{2},\sqrt{3}),a=b+c\sqrt{2}+d\sqrt{3}+e\sqrt{6},b,c,d,e\in\mathbb{Q}$，比如我们可以取 $a=\sqrt{2}+\sqrt{3}$，则 $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$

例 3.13 记 $K=\mathbb{Q}(\sqrt[3]{2},\omega)$，求 $\dim_{\mathbb{Q}}K$

解 考虑域扩张塔 $\mathbb{Q}\subseteq\mathbb{Q}(\sqrt[3]{2})\subseteq\mathbb{Q}(\sqrt[3]{2},\omega)=K$（或可以考虑 $\mathbb{Q}\subseteq\mathbb{Q}(\omega)\subseteq\mathbb{Q}(\omega,\sqrt[3]{2})=K$），则

(1) $\dim_{\mathbb{Q}}\mathbb{Q}(\sqrt[3]{2})$：因为 x^3-2 在 $\mathbb{Q}$ 上零化 $\sqrt[3]{2}$，且素数 $p=2$，由 Eisenstein 判别法知，它在 $\mathbb{Z}[x]$ 上不可约，进而在 $\mathbb{Q}[x]$ 上不可约，则 $\dim_{\mathbb{Q}}\mathbb{Q}(\sqrt[3]{2})=\deg(x^3-2)=3$

(2) $\dim_{\mathbb{Q}(\sqrt[3]{2})}\mathbb{Q}(\sqrt[3]{2},\omega)$，因为 x^2+x+1 在 $\mathbb{Q}(\sqrt[3]{2})$ 上零化 ω，且 x^2+x+1 只有虚根，故它在 $\mathbb{Q}(\sqrt[3]{2})$ 上无根，则它不可约，故 $\dim_{\mathbb{Q}(\sqrt[3]{2})}\mathbb{Q}(\sqrt[3]{2},\omega)=\deg(x^2+x+1)=2$

(3) 由维数公式知 $\dim_{\mathbb{Q}}\mathbb{Q}(\sqrt[3]{2},\omega)=\dim_{\mathbb{Q}}\mathbb{Q}(\sqrt[3]{2})\cdot\dim_{\mathbb{Q}(\sqrt[3]{2})}\mathbb{Q}(\sqrt[3]{2},\omega)=3\times2=6$，因为 $\mathbb{Q}(\sqrt[3]{2})$ 有一组 $\mathbb{Q}$-基 $\{1,\sqrt[3]{2},\sqrt[3]{4}\}$，$\mathbb{Q}(\sqrt[3]{2},\omega)$ 有一组 $\mathbb{Q}(\sqrt[3]{2})$-基 $\{1,\omega\}$，所以 $\mathbb{Q}(\sqrt[3]{2},\omega)$ 有一组 $\mathbb{Q}$-基

$$\{1,\sqrt[3]{2},\sqrt[3]{4},\omega,\sqrt[3]{2}\omega,\sqrt[3]{4}\omega\}$$

Ex 设 K/k 是有限维域扩张，$\alpha\in K$ 在 k 上的最小多项式为 $f(x)$，求证 $\deg f\mid\dim_k K$

Ex P111 1, 4, 7, 10, 11

定义 3.2.2（有限生成的域扩张）称 K/k 有限生成，若 $\exists\alpha_1,\cdots,\alpha_n\in K,\text{s.t. }K=k(\alpha_1,\cdots,\alpha_n)$，此时有域扩张塔

$$k\subseteq k(\alpha_1)\subseteq k(\alpha_1,\alpha_2)\subseteq\cdots\subseteq k(\alpha_1,\cdots,\alpha_n)=K$$

Fact 域扩张 K/k 是有限维的 $\iff$ K/k 是代数扩张，且有限生成

证明 ($\Longrightarrow$)：由引理3.2.1知，K/k 是代数扩张，通过数学归纳法可知 K/k 有限生成

($\Longleftarrow$)：由定义有域扩张塔 $k\subseteq k(\alpha_1)\subseteq k(\alpha_1,\alpha_2)\subseteq\cdots\subseteq k(\alpha_1,\cdots,\alpha_n)=K$，且由代数扩张知 $\dim_{k(\alpha_1),\cdots,k(\alpha_i)}k(\alpha_1,\cdots,\alpha_{i+1})<+\infty$，故

$$\dim_k K=\dim_k k(\alpha_1)\cdot\dim_{k(\alpha_1)}k(\alpha_1,\alpha_2)\cdots\dim_{k(\alpha_1,\cdots,\alpha_{n-1})}k(\alpha_1,\cdots,\alpha_n)<+\infty$$

□

Fact 设有域扩张塔 $k\subseteq E\subseteq K$，则 K/k 是代数扩张 $\iff$ $K/E,E/k$ 均为代数扩张

证明 ($\Longrightarrow$)：根据定义验证即可，由于 K/k 是代数扩张，所以 $\forall\alpha\in K,\exists f(x)\in k[x],\text{s.t. }f(\alpha)=0$，由 $E\subseteq K,k[x]\subseteq E[x]$ 知，$K/E,E/k$ 均为代数扩张

($\Longleftarrow$)：设 $\alpha\in K/k$，若 $\alpha\in E$，由 E/k 是代数扩张知 α 在 k 上代数，下设 $\alpha\in K\backslash E$，因为 K/E 是代数扩张，所以 $\exists u_i\in E,\text{s.t. }\alpha^n+u_{n-1}\alpha^{n-1}+\cdots+u_1\alpha+u_0=0$，设 $E'=k(u_{n-1},\cdots,u_0)\subseteq E$，则 α 是 E' 的代数元，考虑域扩张塔 $k\subseteq E'\subseteq E'(\alpha)$，由上一个 Fact 以及 ($\Longrightarrow$) 知，$E'=k(u_{n-1},\cdots,u_0)$ 是有限生成代数扩张，故 E'/k 是有限维的，另一方面因为 α 在 E' 上代数，所以 $E'(\alpha)/E'$ 是有限维的，进而 $E'(\alpha)/k$ 也是有限维的，由上一个事实知 α 是 k 上的代数元，故 K/k 是代数扩张 □

Fact（代数闭包）对任意域扩张 K/k，定义 $E=\{\alpha\in K|\alpha在K上代数\}$，则 $E\subseteq K$ 是子域，称 E 为 k 在 K 中的代数闭包，此时有域扩张塔 $k\subseteq E\subseteq K$，且 $K\backslash E$ 中没有代数元

证明 只需证明 $\forall\alpha,\beta\in E,\alpha+\beta,\alpha\beta,\alpha^{-1}\in E$，考虑域扩张塔 $k\subseteq k(\alpha)\subseteq k(\alpha,\beta)$，则由上一个事实知，$k(\alpha,\beta)/k$ 是代数扩张，故 $\alpha+\beta,\alpha\beta,\alpha^{-1}$ 在 k 上代数 □

评价 考察域扩张 K/k，若 $\alpha\in K$ 在 k 上的最小多项式为 $f(x),\deg(f(x))=d$，则 α^{-1} 在 k 上的最小多项式为 $x^df(\frac{1}{x})$

例 3.14 考察域扩张 $\mathbb{C}/\mathbb{Q}$，则 $\overline{\mathbb{Q}}=\{\alpha\in\mathbb{C}|\alpha是\mathbb{Q}上的代数元\}$ 是域，称为 $\mathbb{Q}$ 的代数闭包，此时有域扩张塔 $\mathbb{Q}\subseteq\overline{\mathbb{Q}}\subseteq\mathbb{C}$

评价 $\overline{\mathbb{Q}}$ 是可数域，考虑将 $\overline{\mathbb{Q}}$ 中元素与它的最小多项式做对应，注意多项式的根集是有限集

例 3.15 $\overline{\mathbb{R}}=\mathbb{C}$

定义 3.2.3（代数封闭域）称域 K 为代数封闭域，若任意代数扩张 $K\subseteq E$ 均为平凡的，即 $K=E$

命题 3.2.1（代数封闭域的等价表述）

$$\begin{aligned}K是代数封闭域 &\iff 任意不可约多项式f(x)\in K[x],\deg(f)=1\\ &\iff 任意f(x)\in K[x]在K上完全分裂，即f(x)可分解为一次多项式的乘积\end{aligned}$$

Fact 代数封闭域必为无限域

证明 假设 $|K|<+\infty$，则 $f(x)=\prod\limits_{\lambda\in K}(x-\lambda)+1_K\in K[x]$ 在 K 上无根，因此 f 不可分解为 $K[x]$ 上一次多项式的乘积，与 K 是代数封闭域矛盾 □

定理 3.2.2（代数基本定理） $\mathbb{C}$ 是代数封闭域，即 $\forall f(x)\in\mathbb{C}[x]$ 首一，$\exists z_1,\cdots,z_n\in\mathbb{C},\text{s.t. }f(z)=(z-z_1)\cdots(z-z_n)$

§3.3 分裂域

本节关键引理如下

引理 3.3.1（关键引理）

$$\begin{array}{ccc}\alpha\in E & & E'\\ \uparrow & & \uparrow\\ k & \xrightarrow[\sim]{\sigma} & k'\end{array}$$

设有域扩张 $E/k,E'/k'$ 以及域同构 $\sigma:k\xrightarrow{\sim}k'$，设 $\alpha\in E$ 在 k 上的最小多项式 $f(x)=x^n+a_{n-1}x^{n-1}\cdots+a_1x+a_0$，令 $\sigma(f)(x)=x^n+\sigma(a_{n-1})x^{n-1}+\cdots+\sigma(a_1)x+\sigma(a_0)\in k[x]$，由域同态知 $\sigma(f)(x)\in k'[x]$ 不可约，则

(1) 若 $\beta \in \mathrm{Root}_{E'}(\sigma(f))$，即 $\sigma(f)(\beta) = 0_{E'}$，则存在唯一的 σ 的延拓 $\tilde{\sigma}$（即 $\tilde{\sigma}|_k = \sigma$）

$$\begin{aligned} \tilde{\sigma} : k(\alpha) &\xrightarrow{\sim} k'(\beta) \\ \alpha &\longmapsto \beta \end{aligned}$$

(2) 恰有 $|\mathrm{Root}_{E'}(\sigma(f))|$ 个延拓 $\tilde{\sigma} : k(\alpha) \hookrightarrow E'$，使得 $\tilde{\sigma}|_k = \sigma$

评价 $|\mathrm{Root}_{E'}(\sigma(f))| \leq \deg(\sigma(f)) = \deg(f) = \dim_k k(\alpha)$

证明 (1) 至多唯一性：给定 $\beta \in \mathrm{Root}_{E'}(\sigma(f)), \tilde{\sigma}$ 至多唯一，这是因为 $\tilde{\sigma}|_k = \sigma$，且 $k(\alpha)$ 的 k-基 $\{1, \alpha, \cdots, \alpha^{n-1}\}$ 在 $\tilde{\sigma}$ 下的像由 $\tilde{\sigma}(\alpha) = \beta$ 决定，即 $\tilde{\sigma}(\alpha^i) = \beta^i$

存在性：考虑域同态 $\sigma : k \xrightarrow{\sim} k'$ 诱导的环同构（仍记为 σ）$\sigma : k[x] \xrightarrow{\sim} k'[x], x \mapsto x$，我们有理想对应关系 $(f(x)) \longmapsto (\sigma(f)(x))$，进而有环同构（记为 $\overline{\sigma}$，由 $f(x), \sigma(f)(x)$ 不可约知，这是域同构）

$$\begin{aligned} \overline{\sigma} : k[x]/(f(x)) &\longrightarrow k'[x]/(\sigma(f)(x)) \\ \overline{x} &\longmapsto \overline{x} \end{aligned}$$

另一方面，由单扩张结构定理知3.1.2，存在域扩张的同构

$$\begin{aligned} \psi : k[x]/(f(x)) &\longrightarrow k(\alpha) \\ \overline{x} &\longmapsto \alpha \end{aligned} \qquad \begin{aligned} \phi : k'[x]/(\sigma(f)(x)) &\longrightarrow k'(\beta) \\ \overline{x} &\longmapsto \beta \end{aligned}$$

进而我们有域同构 $\tilde{\sigma} = \phi \circ \overline{\sigma} \circ \psi^{-1}$

$$\begin{aligned} \tilde{\sigma} : k(\alpha) &\xrightarrow{\sim} k'(\beta) \\ \alpha &\longmapsto \beta \end{aligned}$$

即下面的图交换

$$\begin{array}{ccc} k(\alpha) & \xleftarrow{\psi} & k[x]/(f(x)) \\ \Big\downarrow{\scriptstyle \tilde{\sigma}} & & \Big\downarrow{\scriptstyle \overline{\sigma}} \\ k'(\beta) & \xleftarrow[\phi]{} & k'[x]/(\sigma(f)(x)) \end{array}$$

(2) 对 $\forall \tilde{\sigma} : k(\alpha) \hookrightarrow E'$，若 $\tilde{\sigma}|_k = \sigma$，由下面的练习知 $\tilde{\sigma}(\alpha) \in \mathrm{Root}_{E'}(\sigma(f))$，且对于每个 $\beta \in \mathrm{Root}_{E'}(\sigma(f))$ 都有唯一一个对应的延拓，故恰有 $|\mathrm{Root}_{E'}(\sigma(f))|$ 个这样的延拓 □

Ex 证明 $\tilde{\sigma}(\alpha) \in \mathrm{Root}_{E'}(\sigma(f))$

定义 3.3.1（分裂域）设 $f(x) \in k[x]$，$f(x)$ 在 k 上的分裂域是指域扩张 E/k 满足

(1) $f(x)$ 在 E 上分裂，即 $f(x)$ 可分解为线性多项式的乘积 $f(x) = (x - \alpha_1) \cdots (x - \alpha_n), \alpha_i \in E, \forall i$

(2) $E = k(\alpha_1, \cdots, \alpha_n)$，即 E 是包含 $\alpha_1, \cdots, \alpha_n$ 的最小子域

评价 考虑域扩张塔 $k \subseteq k(\alpha_1) \subseteq \cdots \subseteq k(\alpha_1, \cdots, \alpha_n)$，由维数公式知 $\dim_k E < +\infty$

Fact $\forall f(x) \in k[x]$ 的分裂域一定存在

证明 Case 1. 若 $f(x)$ 在 k 上分裂，取 $E=k$

Case 2. 设 $f(x)$ 在 k 上有不可约分解 $f(x)=f_1(x)\cdots f_n(x), f_i$ 不可约，$\deg(f_i(x))\geq 2$，取 $E_1=k[x]/(f(x))$，由添根构造知 $f_1(x)$ 在 $K_1[x]$ 上有根 $u=\overline{x}$，故 K_1 中有 $f_1(x)=(x-u)h_1(x)$，则 $f(x)=(x-u)h_1(x)f_2(x)\cdots f_n(x)$ in K_1，对 $f'(x)=h_1(x)f_2(x)\cdots f_n(x)$ 同上操作知，$f(x)$ 的分裂域 E/k 一定存在 □

评价 从上述证明过程中可以看出，$f(x)$ 的分裂域 E/k 不一定存在

例 3.16 设 $f(x)\in\mathbb{Q}[x], f(x)=(x-z_1)\cdots(x-z_n), z_i\in\overline{\mathbb{Q}}$，记 $E=\mathbb{Q}(z_1,\cdots,z_n)\subseteq\overline{\mathbb{Q}}$，则 $E/\mathbb{Q}$ 是 $f(x)$ 的分裂域

例 3.17 $(x^2-2)(x^2-3)\in\mathbb{Q}[x]$ 的分裂域为 $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$

例 3.18 $x^3-2=(x-\sqrt[3]{2})(x-\sqrt[3]{2}\omega)(x-\sqrt[3]{2}\omega^2)\in\mathbb{Q}[x]$ 的分裂域为 $E=\mathbb{Q}(\sqrt[3]{2},\sqrt[3]{2}\omega,\sqrt[3]{2}\omega^2)=\mathbb{Q}(\sqrt[3]{2},\omega)$

Ex 考虑域扩张 $\mathbb{F}_2\hookrightarrow\mathbb{F}_2[x]/(x^2+x+\overline{1})\overset{\text{def}}{=}\mathbb{F}_4$，证明 $\mathbb{F}_4/\mathbb{F}_2$ 是 $x^2+x+\overline{1}\in\mathbb{F}_2[x]$ 的分裂域

Ex 考虑域扩张 $\mathbb{F}_3\hookrightarrow\mathbb{F}_3[x]/(x^2+\overline{1})\overset{\text{def}}{=}\mathbb{F}_9$，证明 $\mathbb{F}_9/\mathbb{F}_3$ 是 $x^2+\overline{1}\in\mathbb{F}_3[x]$ 的分裂域，也是 $x^2+\overline{2}x+\overline{2}\in\mathbb{F}_3[x]$ 的分裂域

定理 3.3.1 给定域同构 $\sigma: k\xrightarrow{\sim}k', f(x)\in k[x], \sigma(f)(x)\in k'[x]$，设 E/k 是 $f(x)$ 的某个分裂域，E'/k' 是 $\sigma(f)(x)$ 的某个分裂域，则 σ 可延拓到域同构 $\delta: E\xrightarrow{\sim}E'$，且 $\delta|_k=\sigma$，这样的域同构 δ 至多有 $\dim_k E=\dim_{k'}E'$ 个

证明 对 $\dim_k E$ 进行归纳

Case 1. 若 $\dim_k E=1$，此时有同构 $k\xrightarrow{\sim}E$，且 $f(x)$ 在 k 上分裂，故 $\sigma(f)(x)$ 在 k' 上分裂，故 E'/k' 平凡，取 $\delta=\sigma$ 即可

Case 2. 若 $\dim_k E>1$，设 $f(x)=(x-\alpha_1)\cdots(x-\alpha_n), \alpha_i\in E,\forall i$，由 $\dim_k E>1$，可不妨设 $\alpha_1\notin k$，则 α_1 在 k 上的最小多项式 $g(x)\in k[x]$ 的次数 $\deg g\geq 2$，且有 $g(x)\mid f(x)$，设 $f(x)=g(x)h(x)$ in $k[x]$ ($g(x)$ 可能等于 $f(x)$)，则 $\sigma(f)=\sigma(g)\sigma(h)$ in $k'[x]$，由 $\sigma(f)$ 在 E' 中分裂知 $\sigma(g)$ 在 E' 中也分裂，故 $\mathrm{Root}_{E'}(\sigma(g)(x))\neq\varnothing$，任取 $\beta_1\in\mathrm{Root}_{E'}(\sigma(g)(x))$，由关键引理知 σ 可延拓至域同构

$$\sigma_1: k(\alpha)\xrightarrow{\sim}k'(\beta_1)$$
$$\alpha_1\longmapsto\beta_1$$

易见 $E/k(\alpha_1)$ 是 $f(x)\in k(\alpha)[x]$ 上的分裂域，$E'/k'(\beta_1)$ 也是 $\sigma(f)(x)$ 在 $k'(\beta_1)[x]$ 上的分裂域，又因为 $\dim_{k(\alpha_1)}E=\frac{\dim_k E}{\dim_k k(\alpha)}<\dim_k E$，由数学归纳法知 σ_1 可延拓至域同构 $\delta: E\xrightarrow{\sim}E'$，且这样的域同构 δ 至多有 $\dim_{k(\alpha_1)}E$ 个，而 σ 延拓得到的 σ_1 至多有 $|\mathrm{Root}_{E'}(\sigma(g))|\leq\deg(g(x))=\dim_k k(\alpha_1)$ 个，故这样的域同构 δ 至多有 $\dim_k k(\alpha_1)\cdot\dim_{k(\alpha_1)}E=\dim_k E$ 个 □

由定理3.3.1立得分裂域的唯一性以及域扩张的自同构群大小的估计

推论 3.3.1 取 $k'=k,\sigma=\mathrm{Id}_k$，则

(1) $f(x)\in k[x]$ 的分裂域在同构意义下唯一

(2) 取 $E=E'$，则 $|\mathrm{Aut}(E/k)|\leq\dim_k E$

例 3.19 由例3.13和例3.18知 $x^3-2\in\mathbb{Q}[x]$ 的分裂域为 $E=\mathbb{Q}(\sqrt[3]{2},\omega),\dim_{\mathbb{Q}}E=6$，求 $\mathrm{Aut}(E/\mathbb{Q})=\mathrm{Aut}(E)$（这是因为 $\mathbb{Q}$ 上的自同构只有 $\mathrm{Id}_{\mathbb{Q}}$）

解 首先有 $|\mathrm{Aut}(E)|\le\dim_{\mathbb{Q}}E=6$，考虑域扩张塔 $\mathbb{Q}\subseteq\mathbb{Q}(\sqrt[3]{2})\subseteq\mathbb{Q}(\sqrt[3]{2},\omega)=E$

(1) 因为 $\mathrm{Root}_E(x^3-2)=\{\sqrt[3]{2},\sqrt[3]{2}\omega,\sqrt[3]{2}\omega^2\}$，所以 $\mathrm{Id}_{\mathbb{Q}}$ 有三个延拓

- $\beta_1=\sqrt[3]{2},\sigma_1:\mathbb{Q}(\sqrt[3]{2})\to\mathbb{Q}(\sqrt[3]{2}),\sqrt[3]{2}\mapsto\sqrt[3]{2}$
- $\beta_2=\sqrt[3]{2}\omega,\sigma_2:\mathbb{Q}(\sqrt[3]{2})\to\mathbb{Q}(\sqrt[3]{2}\omega),\sqrt[3]{2}\mapsto\sqrt[3]{2}\omega$
- $\beta_3=\sqrt[3]{2}\omega^2,\sigma_3:\mathbb{Q}(\sqrt[3]{2})\to\mathbb{Q}(\sqrt[3]{2}\omega^2),\sqrt[3]{2}\mapsto\sqrt[3]{2}\omega^2$

(2) 在 $\mathbb{Q}(\sqrt[3]{2})$ 上，ω 的最小多项式为 x^2+x+1，因为 $\mathrm{Root}_E(x^2+x+1)=\{\omega,\omega^2\}$，所以每个 $\sigma_i,i=1,2,3$ 均有两个延拓，记为 $\delta_{ij},j=1,2$，具体如下

- σ_1 有两个延拓 $\delta_{11}:E\to E,\omega\mapsto\omega,\delta_{12}:E\to E,\omega\mapsto\omega^2$
- σ_2 有两个延拓 $\delta_{21}:E\to E,\omega\mapsto\omega,\delta_{22}:E\to E,\omega\mapsto\omega^2$
- σ_3 有两个延拓 $\delta_{31}:E\to E,\omega\mapsto\omega,\delta_{32}:E\to E,\omega\mapsto\omega^2$

进而我们有 $\delta_{ij}\in E,i=1,2,3,j=1,2$，且由 $|\mathrm{Aut}(E)|=6$ 知，$\mathrm{Aut}(E)=\{\delta_{ij}|i=1,2,3,j=1,2\}$，以 $\mathrm{Id}_{\mathbb{Q}}\to\sigma_2\to\delta_{22}$ 为例，有交换图如下

$$\begin{array}{ccc}
E=\mathbb{Q}(\sqrt[3]{2})(\omega) & \xrightarrow[\delta_{22}:\omega\mapsto\omega^2]{\sim} & E=\mathbb{Q}(\sqrt[3]{2}\omega)(\omega^2)\\
\uparrow & & \uparrow\\
\mathbb{Q}(\sqrt[3]{2}) & \xrightarrow[\sigma_2:\sqrt[3]{2}\mapsto\sqrt[3]{2}\omega]{\sim} & \mathbb{Q}(\sqrt[3]{2}\omega)\\
\uparrow & & \uparrow\\
\mathbb{Q} & \xlongequal{\quad\mathrm{Id}_{\mathbb{Q}}\quad} & \mathbb{Q}
\end{array}$$

Ex 求 $\delta_{ij}^{-1},i=1,2,3,j=1,2$，并求 $\mathrm{Aut}(E)$ 的乘法表

Ex 仿照上面过程，求

(1) $\mathrm{Aut}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$

(2) $\mathrm{Aut}(\mathbb{F}_4/\mathbb{F}_2)$，这里 $\mathbb{F}_4\overset{\mathrm{def}}{=}\mathbb{F}_2/(x^2+x+\overline{1})$

Ex 证明

(1) $|\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})|<\dim_{\mathbb{Q}}\mathbb{Q}(\sqrt[3]{2})$

(2) 证明不存在 $\delta:\mathbb{Q}(\sqrt[4]{2})\to\mathbb{Q}(\sqrt[4]{2})$ 使得图交换

$$\begin{array}{ccc}
\mathbb{Q}(\sqrt[4]{2}) & \xrightarrow{\nexists\delta} & \mathbb{Q}(\sqrt[4]{2})\\
\uparrow\theta & & \uparrow\theta\\
\mathbb{Q}(\sqrt{2}) & \xrightarrow{\sigma} & \mathbb{Q}(\sqrt{2})
\end{array}$$

其中 $\sigma(a+b\sqrt{2})=a-b\sqrt{2}$

结合定理3.3.1，我们知道 σ 的延拓至多有 $\dim_k E$ 个，结合上面的习题知这不一定取等，接下来我们讨论何时取等，即 σ 的延拓何时有 $\dim_k E$ 个

定义 3.3.2（重根）称 $0 \neq f(x) \in k[x]$ 有重根，若存在域扩张 E/k 和 $a \in E, \text{s.t. } (x-a)^2 \mid f(x)$

评价 (1) $(x-a)^2$ 不一定在 $k[x]$ 中

(2) $f(x) \in k[x]$ 无重根指的是对任意域扩张 E/k，$f(x)$ 在 $E[x]$ 中均不存在二重线性因子

例 3.20 $f(x) = (x^2+1)^2 \in \mathbb{R}[x]$ 有重根

Ex 设 $k = \mathbb{F}_p(t)$，证明 $f(x) = x^p - t \in k[x]$ 不可约，但是有重根

定义 3.3.3（形式微商）设 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in k[x]$，称

$$f'(x) = na_n x^{n-1} + \cdots + a_1 \in k[x]$$

为 $f(x)$ 的形式微商

评价 $\deg(f'(x)) \leq \deg(f(x)) - 1$，可以不取等，考虑 $k = \mathbb{F}_p, f(x) = x^p \in k[x]$

定理 3.3.2（Leibniz 法则）对 $\forall f(x), g(x) \in k[x]$，则

$$\big(f(x)g(x)\big)' = f'(x)g(x) + g'(x)f(x)$$

引理 3.3.2 $f(x) \in k[x]$ 有重根 $\iff \gcd_{k[x]}(f, f') \neq 1$

证明 ($\Longrightarrow$)：设 $k \hookrightarrow E$，在 E 中有 $f(x) = (x-a)^2 h(x)$，则 $f'(x) = 2(x-a)h(x) + (x-a)^2 h'(x)$，所以 $x - a \mid \gcd(f, f')$，进而 $\gcd_{k[x]}(f, f') \neq 1$

($\Longleftarrow$)：设 $\gcd_{k[x]}(f, f') = g(x) \neq 1$，取 K 为 $g(x)$ 的分裂域，则 $\exists a \in K, \text{s.t. } x - a \mid g(x) \text{ in } K[x]$，故在 $K[x]$ 中可设 $f(x) = (x-a)h(x)$，所以 $f'(x) = h(x) + (x-a)h'(x) \text{ in } K[x]$，由 $x - a \mid f'(x)$ 知，$x - a \mid h(x)$，进而 $(x-a)^2 \mid h(x) \text{ in } K[x]$ □

推论 3.3.2 $f(x) \in k[x]$ 无重根 $\iff \gcd_{k[x]}(f, f') = 1$

定义 3.3.4（可分）称 $f(x) \in k[x]$ 在 k 上可分，若 $f(x)$ 的不可约因子均无重根

Ex 设有域扩张 K/k，若 $f(x) \in k[x]$ 在 k 上可分，则 $f(x)$ 在 K 上也可分

命题 3.3.1 若 $\text{Char}(k) = 0$，则 $\forall f(x) \in k[x]$ 可分

证明 只需证明任意 $k[x]$ 上的不可约多项式 $f(x)$ 均无重根，设 $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in k[x]$ 不可约，由 $\text{Char}(k) = 0$ 知，$na_n \neq 0$，故 $\deg(f') = \deg(f) - 1$，且 $f(x)$ 非常值多项式，$f'(x) \neq 0$，由带余除法知

$$\gcd_{k[x]}(f.f') = 1$$

由推论3.3.2知，$f(x)$ 在 k 上可分 □

接下来我们可以回答：σ 的延拓有 $\dim_k E$ 个的充要条件是 $f(x)\in k[x]$ 可分

定理 3.3.3 设 $f(x)\in k[x]$，E 为 f 的分裂域，则 $f(x)$ 在 k 上可分 $\iff |\mathrm{Aut}(E/k)|=\dim_k E$

证明 ($\Longrightarrow$)：对 $|\mathrm{Aut}(E/k)|$ 归纳，$|\mathrm{Aut}(E/k)|=1$ 时平凡，当 $|\mathrm{Aut}(E/k)|\geq 2$ 时，设 $f(x)=(x-\alpha_1)\cdots(x-\alpha_n)$，由 $|\mathrm{Aut}(E/k)|\geq 2$ 知，可不妨设 $\alpha_1\notin k$

$$\begin{array}{ccc} E & \xhookrightarrow{\bar{\delta}} & E \\ \uparrow & & \uparrow \\ k(\alpha_1) & \xrightarrow[\alpha_1\mapsto\beta]{\delta} & k(\beta) \\ \uparrow & & \uparrow \\ k & = & k \end{array}$$

设 α_1 在 k 上的最小多项式为 $g(x)$，则 $g(x)$ 不可约且由 $f(x)$ 可分，$g(x)\mid f(x)$ 知 $g(x)$ 无重根，故 $|\mathrm{Root}_E(g(x))|=\deg(g(x))$，类似关键引理的证明知 Id_k 共有 $|\mathrm{Root}_E(g(x))|=\deg(g(x))$ 个延拓，又因为 $f(x)$ 在 k 上可分 $\Longrightarrow f(x)$ 也在 $k(\alpha_1)$ 上可分，故给定 Id_k 的延拓 $\sigma: k(\alpha_1)\to k(\beta)$，其中 $\beta\in\mathrm{Root}_E(g(x))$，由数学归纳法知 σ 共有 $\dim_{k(\alpha_1)}E$ 个延拓，而这样的 σ 共有 $\deg(g(x))=\dim_k k(\alpha_1)$ 个，因此

$$|\mathrm{Aut}(E)/k|=\dim_k k(\alpha_1)\cdot\dim_{k(\alpha_1)}E=\dim_k E$$

($\Longleftarrow$)：反证，假设 $f(x)\in k[x]$ 在 k 上不可分，则存在某个 α_i，它在 k 上的最小多项式 $g(x)$ 有重根，不妨设为 α_1，则同上过程知 Id_k 到 $k(\alpha_1)$ 的延拓个数为 $|\mathrm{Root}_E(g(x))|<\deg(g(x))=\dim_k k(\alpha_1)$，因此

$$\dim_k E=\dim_k k(\alpha_1)\cdot\dim_{k(\alpha_1)}E>|\mathrm{Id}_k\text{到}k(\alpha_1)\text{的延拓}|\cdot\dim_{k(\alpha_1)}E\geq|\mathrm{Aut}(E/k)|$$

这与 $|\mathrm{Aut}(E/k)|=\dim_k E$ 矛盾！ □

§3.4 有限域

有限域指的是阶有限的域，由于域是整环，整环的特征为零或素数 p，且特征为零的域一定是无限域，故若 $|E|<+\infty$，则存在素数 p 使得 $\mathrm{Char}(E)=p$

Fact 若 $\mathrm{Char}(E)=p$，则 $\forall a\in E, pa=0_E$

命题 3.4.1（有限域的阶）设 E 为有限域，则存在唯一素数 p 以及特征同态

$$\begin{aligned}\varphi:\mathbb{F}_p &\hookrightarrow E\\ \overline{1} &\longmapsto 1_E\end{aligned}$$

因此有域扩张 $E/\mathbb{F}_p$，且 E 是 $\mathbb{F}_p$-线性空间，由 $|E|<+\infty$ 知，可设 $\dim_{\mathbb{F}_p}E=n$，则有线性同构 $E\simeq\mathbb{F}_{p^n}$，即 $|E|=p^n$

评价 当 $n=1$ 时，$E \simeq \mathbb{F}_p$

定义 3.4.1（Frobenius 自同构）设 $\mathrm{Char}(E)=p$，称

$$\begin{aligned} \sigma : E &\longrightarrow E \\ a &\longmapsto a^p \end{aligned}$$

为 E 上的 Frobenius 自同构，以下的 σ 均指 Frobenius 自同构

Fact $\sigma \in \mathrm{Aut}(E)$，即 Frobenius 自同构确实是域自同构

证明 验证同态，乘法显然，对于加法

$$\sigma(a+b)=(a+b)^p=a^p+\binom{p}{1}a^{p-1}b+\cdots+\binom{p}{p-1}ab^{p-1}+b^p=a^p+b^p=\sigma(a)+\sigma(b)$$

下验证双射，因为 $|E|=|E|$，故只需验证单射，若 $\sigma(a)=\sigma(b)$，则 $\sigma(a-b)=(a-b)^p=0 \Longrightarrow a-b=0$，即 $a=b$

□

评价 Fermat 小定理：若 $(a,p)=1$，则 $a^p \equiv a \mod p$，因此 $\sigma|_{\mathbb{F}_p}=\mathrm{Id}_{\mathbb{F}_p}$

例 3.21 考虑 $\mathbb{F}_4=\mathbb{F}_2[x]/(x^2+x+\overline{1})=\begin{Bmatrix} \overline{0} & \overline{1} \\ u & u+\overline{1} \end{Bmatrix}$，则

$$\begin{cases} \sigma|_{\mathbb{F}_2}=\mathrm{Id}_{\mathbb{F}_2} \\ \sigma(u)=u^2=u+\overline{1} \\ \sigma(u+1)=u^2+\overline{1}=u \end{cases} \Longrightarrow \sigma^2=\mathrm{Id}_{\mathbb{F}_4}$$

由于 $|\mathrm{Aut}(\mathbb{F}_4/\mathbb{F}_2)| \le \dim_{\mathbb{F}_2}\mathbb{F}_4=\deg(x^2+x+\overline{1})=2$，且有 $\mathrm{Id}_{\mathbb{F}_4}, \sigma \in \mathrm{Aut}(\mathbb{F}_4/\mathbb{F}_2)$，故

$$\mathrm{Aut}(\mathbb{F}_4/\mathbb{F}_2)=\{\mathrm{Id}_{\mathbb{F}_4}, \mathrm{Aut}(\mathbb{F}_4/\mathbb{F}_2)\}$$

Ex 考虑 $\mathbb{F}_9=\mathbb{F}_3[x]/(x^2+\overline{1})=\begin{Bmatrix} \overline{0} & \overline{1} & \overline{2} \\ u & u+\overline{1} & u+\overline{2} \\ \overline{2}u & \overline{2}u+\overline{1} & \overline{2}u+\overline{2} \end{Bmatrix}$，证明 $\mathrm{Aut}(\mathbb{F}_9/\mathbb{F}_3)=\{\mathrm{Id}_{\mathbb{F}_9}, \sigma\}$

Fact 设 $|E|=p^n$，定义 $E^\times=E\backslash\{0_E\}$ 为 E 的单位群，我们有 $|E^\times|=p^n-1$

引理 3.4.1 对 $\forall a \in E^\times$，总有 $a^{p^n-1}=\overline{1}$ 或 $a^{p^n}=a$

证明 考虑

$$(a)=\{1, a, a^2, \cdots, a^m, \cdots\}$$

由 $|E|<+\infty$ 知，一定 $\exists i<j, \text{s.t. } a^i=a^j$，故 $a^{j-i}=\overline{1}$，取 $d=\min\{m|a^m=\overline{1}\}$，则 $\{1, a, a^2, \cdots, a^{d-1}\}$ 两两不同，且为 $E^\times$ 的子群，由群论的 Lagrange 定理4.1.2，$d \mid p^n-1$，所以 $a^{p^n-1}=\overline{1}$ □

推论 3.4.1 $\sigma^n = \mathrm{Id}_E$

证明 对 $\forall a \in E$

$$\sigma^n(a) = (((a)^p)^p \cdots)^p = a^{p^n} = a$$

□

定理 3.4.1 对 $\forall n \in \mathbb{N}^*$ 以及素数 p，存在唯一 p^n 阶有限域，记作 $\mathbb{F}_{p^n}$

证明 至多唯一性：若 $E = p^n$，我们断言 $E/\mathbb{F}_p$ 是 $x^{p^n} - x \in \mathbb{F}_p[x]$ 的分裂域

Proof Of Claim : $\forall a \in E, a \in \mathrm{Root}_E(x^{p^n} - x)$，即

$$x^{p^n} - x = \prod_{a \in E}(x - a) \text{ in } E[x]$$

又因为 $x^{p^n} - x$ 的分裂域至少包含它的所有根（且它的 p^n 个根两两不同），即有 p^n 个元素，且 $|E| = p^n$ 满足分裂域的最小性，故 $E/\mathbb{F}_p$ 是 $x^{p^n} - x \in \mathbb{F}_p[x]$ 的分裂域，由分裂域在同构意义下唯一即证

存在性：设 $E/\mathbb{F}_p$ 为 $x^{p^n} - x$ 的分裂域，由引理3.2.1知 $E/\mathbb{F}_p$ 是有限维域扩张，故 $|E| < +\infty$，我们取 $K = \{a \in E | a^{p^n} = a\} = \{a \in E | \sigma^n(a) = a\}$，只需证明如下断言

(1) $K \subseteq E$ 是子域

(2) $x^{p^d} - x$ 无重根

(3) $K = E$

□

Ex 补全上面的证明

推论 3.4.2 给定 $\mathbb{F}_{p^n}$，我们有

$$x^{p^n} - x = \prod_{a \in \mathbb{F}_{p^n}}(x - a)$$

评价 特别地，当 $n = 1$ 时，$x^p - x = x(x - \overline{1}) \cdots (x - \overline{p-1})$ 或 $x^{p-1} - x = (x - \overline{1}) \cdots (x - \overline{p-1})$，取 $x = \overline{0}$ 即得 Wilson 定理

$$(p-1)! \equiv -1 \mod p$$

命题 3.4.2 在 $\mathbb{F}_p[x]$ 中有

$$x^{p^n} - x = \prod_{d|n} \prod_{\substack{\deg(f)=d \\ f \text{ 首一不可约} \\ \text{每个只出现一次}}} f(x)$$

证明 一方面，取 $f(x) \in \mathbb{F}_p[x]$ 不可约，且 $f(x) \mid x^{p^n} - x$，下证 $\deg d \mid n$：因为 $f(x)$ 在 $\mathbb{F}_{p^n}$ 中分裂，所以 $\exists a \in \mathbb{F}_{p^n}, \text{s.t. } f(a) = 0$，考虑域扩张塔

$$\mathbb{F}_p \subseteq \mathbb{F}_p(a) \subseteq \mathbb{F}_{p^n}$$

由维数公式知 $\deg(f)=\dim_{\mathbb{F}_p}\mathbb{F}_p(a)\mid\dim_{\mathbb{F}_p}\mathbb{F}_{p^n}=n$

另一方面，对于 $\forall d\mid n,\forall d$ 次首一不可约多项式 $g(x)\in\mathbb{F}_p[x]$，下证 $g(x)\mid x^{p^n}-x$：考虑添根构造 $\mathbb{F}_p\hookrightarrow\mathbb{F}_p/(g(x))\overset{\text{def}}{=}K$，因为 $\dim_{\mathbb{F}_p}K=\deg(g(x))=d$，所以 $|K|=p^d$，由引理3.4.1知，$\overline{x}\overset{\text{def}}{=}u\in K$ 满足 $u^{p^d}-u=0$，且 $g(x)$ 为 u 的最小多项式，故

$$g(x)\mid x^{p^d}-x\mid x^{p^n}-x$$

□

例 3.22 当 $p=2$ 时，取 $n=2,3,4$，则

- $x^{2^2}-x=x(x+\overline{1})(x^2+x+\overline{1})$
- $x^{2^3}-x=x(x+\overline{1})(x^3+x^2+\overline{1})(x^3+x+\overline{1})$
- $x^{2^4}-x=x(x+\overline{1})(x^2+x+\overline{1})(x^4+x+\overline{1})(x^4+x^3+x+1)(x^4+x^3+x^2+x+\overline{1})$

Ex 在 $\mathbb{F}_3[x]$ 中分解 $x^{3^2}-x$

命题 3.4.3（有限域的子域）取定有限域 $E,|E|=p^n$，则

(1) 若 $K\subseteq E$ 是子域，则 $\exists d\mid n,\text{s.t. }|K|=p^d$

(2) 对 $\forall d\mid n$，存在唯一 p^d 阶子域 $K\subseteq E$

(3) 记 E 的 p^d 阶子域为 K_d，则 $K_{d_1}\subseteq K_{d_2}\iff d_1\mid d_2$

证明 (1) 考虑域扩张塔 $\mathbb{F}_p\subseteq K\subseteq E$，由维数公式易证

(2) 至多唯一性：设有子域 $K\subseteq E$ 满足 $|K|=p^d$，则由引理3.4.1知 $\forall a\in K,a^{p^d}-a=0$，则 $K\subseteq\text{Root}_E(x^{p^d}-x)$，因为 $x^{p^d}-x\mid x^{p^n}-x$，且两边元素一样，故 $K=\text{Root}_E(x^{p^d}-x)$ 存在性：取 $K=\text{Root}_E(x^{p^d}-x)=\{a\in E|a^{p^d}=a\}=\{a\in E|\sigma^d(a)=a\}$，只需证明如下断言

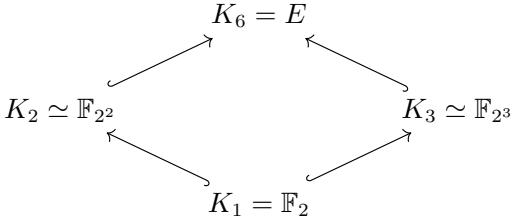
- $x^{p^d}-x$ 在 E 上分裂
- $x^{p^d}-x$ 无重根
- K 是子域

(3) 这是自然的推论

□

Ex 补全上面的证明

例 3.23 $|E|=2^6$，记 $K_6=E,K_1=\mathbb{F}_2$，由命题3.4.3知 E 存在唯一 $2^2,2^3$ 阶子域 $K_2=\text{Root}_E(x^{2^2}-x),K_3=\text{Root}_E(x^{2^3}-x)$



Ex 设 $|E|=\mathbb{F}_{p^n}$，n 有素因子分解 $n=p_1^{e_1}\cdots p_s^{e_s}$，则 E 有 s 个极大真子域 $K_{\frac{n}{p_i}},|K_{\frac{n}{p_i}}|=p^{\frac{n}{p_i}}$，求证

$$\left|\bigcup_{i=1}^{s}K_{\frac{n}{p_i}}\right|<|E|$$

推论 3.4.3 $\mathbb{F}_{p^n}/\mathbb{F}_p$ 是单扩张，且 $\mathbb{F}_p[x]$ 上总有 n 次不可约多项式

证明 由上面的练习，任取 $u \in E \setminus \bigcup_{i=1}^{s} K_{\frac{n}{p_i}}$，我们有 $\mathbb{F}_{p^n} = \mathbb{F}_p(u)$，即 $\mathbb{F}_{p^n}/\mathbb{F}_p$ 是单扩张，且 u 在 $\mathbb{F}_p[x]$ 上的最小多项式次数为 n □

Ex 设 $|E| = p^n$，记 E 的 p^d 阶子域为 K_d，求证

(1) $K_{d_1} \cap K_{d_2} = K_{\gcd(d_1,d_2)}$

(2) 记 $K_{d_1} \vee K_{d_2}$ 为包含 $K_{d_1} \cup K_{d_2}$ 的最小子域，则 $K_{d_1} \vee K_{d_2} = K_{\mathrm{lcm}(d_1,d_2)}$

命题 3.4.4

$$\mathrm{Aut}(E/\mathbb{F}_p) =< \sigma >$$

证明 因为 $\mathbb{F}_p$ 上的自同构只有 $\mathrm{Id}_{\mathbb{F}_p}$，所以 $\mathrm{Aut}(E/\mathbb{F}_p) = \mathrm{Aut}(E)$，且由推论3.4.1知 $\sigma^n = \mathrm{Id}_E$，下证 $\{\mathrm{Id}_E, \sigma, \cdots, \sigma^{n-1}\}$ 两两不同，取3.4.3证明过程中的 $u \in E$，我们断言 $\{u, \sigma(u), \cdots, \sigma^{n-1}(u)\}$ 两两不同

Proof Of Claim : 只需证 $\forall 1 \le i \le n-1, \sigma^i(u) \ne u$

如不然，取最小的 $d \le n-1, \text{s.t. } \sigma^d(u) = u$，设 $n = qd + r, r < d$，则

$$u = \sigma^n(u) = \sigma^r \circ \overbrace{\sigma^d \circ \cdots \circ \sigma^d}^{q\text{个}}(u) = \sigma^r(u)$$

由 d 的最小性知 $r = 0$，故 $d \mid n$，但此时有 $u \in \mathrm{Root}_E(x^{p^d} - x) = K^d$，这与 u 的取法矛盾！进而有 $\forall 0 \le i < j \le n-1, \sigma^i(u) \ne \sigma^j(u)$，即断言得证，则 $\{\mathrm{Id}_E, \sigma, \cdots, \sigma^{n-1}\}$ 两两不同，由于 $|\mathrm{Aut}(E/\mathbb{F}_p)| \le n$，且 $< \sigma > \subseteq \mathrm{Aut}(E/\mathbb{F}_p)$，所以 $\mathrm{Aut}(E/\mathbb{F}_p) =< \sigma >$ □

命题 3.4.5 设 $|E| = p^n$，对 n 次不可约多项式 $f(x) \in \mathbb{F}_p[x]$，取 $u \in \mathrm{Root}_E(f(x))$，则

$$f(x) = \prod_{i=0}^{n-1}(x - \sigma^i(u))$$

证明 同3.4.4的证明知 $\sigma^i(u), 0 \le i \le n-1$ 两两不同，且它们均为 $f(x)$ 的根 □

评价 此时 E 也是 n 次不可约多项式 $f(x)$ 的分裂域

Fact 对 $\forall d \mid n$，记

$$H_d = \{\mathrm{Id}_E, \sigma^d, \cdots, \sigma^{n-d}\} =< \sigma^d >$$

则 H_d 是 $\mathrm{Aut}(E)$ 的子群，且它是 $\mathrm{Aut}(E)$ 唯一的 $\frac{n}{d}$ 阶子群 H_d

定理 3.4.2（有限域的 Galois 对应）取定有限域 $E, |E| = p^n$，则存在双射

$$\{K | K \overset{\text{子域}}{\subseteq} E\} \overset{1:1}{\longleftrightarrow} \{\mathrm{Aut}(E)\text{的子群}\}$$
$$K_d \longmapsto H_d$$

评价 实际上

$$H_d = \mathrm{Aut}(E/K_d) = \{\delta \in \mathrm{Aut}(E) : \delta|_{K_d} = \mathrm{Id}_{K_d}\}$$

§3.5 分圆域

定义 3.5.1（单位根）设 k 是域，称 $\omega \in k$ 是 n 次单位根，若 $\omega^n = 1_k$，若 d 是最小的正整数使得 $\omega^d = 1_k$，则称 ω 为 d 次本原单位根，且记 $d = \mathrm{Ord}(\omega)$

Fact 设 $\mathrm{Ord}(\omega) = d$，则

(1) $\omega^n = 1_k \iff d \mid n$

(2) $k^\times = k\backslash\{0_k\}$ 有 d 阶子群 $\mathrm{Root}_k(x^d - 1) = \{1, \omega, \cdots, \omega^{d-1}\} \leq k^\times$

Ex 设 $\mathrm{Ord}(\omega) = d, \mathrm{Char}(k) = p > 0$，证明 $p \nmid d$

定理 3.5.1 对任意域 k，任意 d 阶子群 $H \leq k^\times$，存在 d 次本原单位根 ω, s.t.

$$H = \{1, \omega, \cdots, \omega^{d-1}\} =< \omega >$$

且这样的 H 唯一

证明 至多唯一性：$H = \mathrm{Root}_k(x^d - 1)$

存在性：即证明 H 是循环群，小伍：难！我们先承认它 □

推论 3.5.1 设 E 是有限域，$|E| = p^n$，则 $E^\times = E\backslash\{0_E\}$ 是 $p^n - 1$ 阶循环群，因为存在 $p^n - 1$ 次本原单位根 $\omega \in E^\times$，此时有

(1) $E^\times = \{1, \omega, \cdots, \omega^{p^n - 2}\}$

(2) $\mathbb{F}_p(\omega) = E$

定义 3.5.2（复单位根）对 $\forall n \geq 2$，定义 $\zeta = \zeta_n = e^{\frac{2\pi i}{n}}$，则

$$\mathrm{Root}_{\mathbb{C}}(x^n - 1) = \{1, \zeta, \cdots, \zeta^{n-1}\} \leq \mathbb{C}^x$$

是 $\mathbb{C}^x$ 唯一的 n 阶子群

Fact（复）n 次本原单位根共有 $\phi(n)$ 个

证明 这是因为 $\forall 1 \leq m < n, \mathrm{Ord}(\zeta^m) = \frac{n}{\gcd(m,n)}$ □

定义 3.5.3（分圆域）这 ζ_n 为 n 次复单位根，则 $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ 恰为 $x^n - 1$ 的分裂域，称为第 n 个分圆域

例 3.24 $\mathbb{Q}(\zeta_2) = \mathbb{Q}$

$\mathbb{Q}(\zeta_3)=\mathbb{Q}\left(\frac{-1+\sqrt{-3}}{2}\right)=\mathbb{Q}(\sqrt{-3})$
$\mathbb{Q}(\zeta_4)=\mathbb{Q}(\sqrt{-1})$
$\mathbb{Q}(\zeta_5)\supset\mathbb{Q}(\sqrt{5})$

定义 3.5.4（分圆多项式）称

$$\Phi_n(x)=\prod_{\omega\text{是 }n\text{ 次本原}}(x-\omega)=\prod_{\substack{1\le m\le n-1\\ \gcd(m,n)=1}}(x-\zeta_n^m)$$

为第 n 个分圆多项式，补充定义 $\Phi_1(x)=x-1$，由表达式易知 $\deg(\Phi_n(x))=\phi(n)$

引理 3.5.1

$$x^n-1=\prod_{d|n}\Phi_d(x)\ \text{或}\ \Phi_n(x)=\frac{x^n-1}{\prod\limits_{\substack{d<n\\ d|n}}\Phi_d(x)}$$

证明 记 $S_d=\{\zeta_n^{\frac{n}{d}\cdot k}|1\le k\le d,\gcd(d,k)=1\}$ 为 d 次单位根的集合，因为 $\forall k,\mathrm{Ord}(\zeta_n^k)\mid n$，且我们有分拆 $\{1,\zeta_n,\cdots,\zeta_n^{n-1}\}=\bigsqcup\limits_{d|n}S_d$，所以

$$x^n-1=\prod_{i=0}^{n-1}(x-\zeta_n^i)=\prod_{d|n}\prod_{\omega\in S_d}(x-\omega)=\prod_{d|n}\Phi_d(x)$$

例 3.25 $\Phi_2(x)=\frac{x^2-1}{x-1}=x+1$
$\Phi_3(x)=\frac{x^3-1}{x-1}=x^2+x+1$
$\Phi_4(x)=\frac{x^4-1}{(x-1)(x+1)}=x^2+1$
对于素数 p，$\Phi_p(x)=\frac{x^p-1}{x-1}=x^{p-1}+\cdots+x+1$

Fact $\forall n\in\mathbb{N}^*,\Phi_n(x)\in\mathbb{Z}[x]$

证明 $n=1$ 时 $\Phi_1(x)=x-1\in\mathbb{Z}[x]$，当 $n>1$ 时，使用数学归纳法，设 $\forall m<n,\Phi_m(x)\in\mathbb{Z}[x]$，下证 $\Phi_n(x)\in\mathbb{Z}[x]$，因为 $\Phi_n(x)=\frac{x^n-1}{\prod\limits_{\substack{d<n\\ d|n}}\Phi_d(x)}$，且 $f(x)\overset{\text{def}}{=}\prod\limits_{\substack{d<n\\ d|n}}\Phi_d(x)\in\mathbb{Z}[x]$，且 $f(x)\Phi_n(x)=x^n-1$，由下面的练习知 $\Phi_n(x)\in\mathbb{Z}[x]$

□

Ex 设 $f(x),g(x)\in\mathbb{Z}[x],g(x)$ 首一，若 $f(x)=g(x)h(x),g(x)\in\mathbb{C}[x]$，证明 $h(x)\in\mathbb{Z}[x]$

定理 3.5.2（Gauss/Kronecker）分圆多项式 $\Phi_n(x)\in\mathbb{Z}[x]$ 不可约

证明 取 ζ_n 的最小多项式 $f(x)\in\mathbb{Z}[x]$，则 $f(x)$ 本原且 $f(x)\mid\Phi_n(x)$ in $\mathbb{Q}[x]$

***Claim*:** 若素数 $p\nmid n$，若 $f(z)=0$，则 $f(z^p)=0$

Proof Of Claim : 反证法，假设 $f(z^p)\neq 0$，设 z^p 的最小多项式 $g(x)\in\mathbb{Z}[x]$，则 $g(x)$ 本原，由 f,g 不可约，且 $f\neq g$ 知，$\gcd(f,g)=1$，因此可设 $x^n-1=f(x)g(x)h(x)$；此外我们有 $g(z^p)=0\Longrightarrow z$ 被 $g(x^p)$ 零化 $\Longrightarrow f(x)\mid g(x^p)$，考虑模 p 约化

$$\begin{aligned}\psi:\mathbb{Z}[x]&\longrightarrow \mathbb{F}_p[x]\\ x&\longmapsto x\\ a&\longmapsto \overline{a}\end{aligned}$$

设 $g(x)=b_mx^m+\cdots+b_1x+b_0$，则

$$\begin{aligned}\psi(g(x^p))&=\overline{b}_m^px^{pm}+\cdots+\overline{b}_1^px^p+\overline{b}_0^p\\&=\overline{b}_mx^{pm}+\cdots+\overline{b}_1x^p+\overline{b}_0\end{aligned}$$

$$\begin{aligned}\psi(g(x))^p&=(\overline{b}_mx^m)^p+\cdots+(\overline{b}_1x)^p+\overline{b}_0^p\\&=\overline{b}_mx^{pm}+\cdots+\overline{b}_1x^p+\overline{b}_0\end{aligned}$$

所以 $\psi(g(x^p))=\psi(g(x))^p$，由 $f(x)\mid g(x^p)$ 知，$\psi(f(x)),\psi(g(x^p))=\psi(g(x))^p$ 有相同的不可约因子，设为 $a(x)$，所以

$$\begin{cases}a(x)\mid\psi(f(x))\mid\psi(x^n-1)\\ a(x)\mid\psi(g(x))^p\mid\psi(x^n-1)\end{cases}$$

即 $\psi(x^n-1)=x^n-1\in\mathbb{F}_p[x]$ 有重根，但是 $\gcd(x^n-1,\overline{n}x^{n-1})=1$，矛盾！

因此断言得证，下面证明每个本原单位根 $\zeta_n^k,\gcd(n,k)=1$ 均为 $f(x)$ 的根，对 k 做素因子分解 $k=p_1\cdots p_s$（相同素数可以重复出现），由 $\gcd(n,k)=1$ 知 $p_i\nmid n$，反复利用断言

$$f(\zeta_n)=0\Longrightarrow f(\zeta_n^{p_1})=0\Longrightarrow f(\zeta_n^{p_1p_2})=0\Longrightarrow\cdots\Longrightarrow f(\zeta_n^{p_1\cdots p_s})=f(\zeta_n^k)=0$$

所以 $\deg(f(x))=\phi(n)=\deg(\Phi_n(x))$，又因为 $f(x)\mid\Phi_n$，所以 $f(x)=\Phi_n(x)$，即 $\Phi_n(x)\in\mathbb{Z}[x]$ 不可约 □

评价 由上述证明过程知，$\Phi_n(x)$ 是任意本原单位根 $\zeta_n^k,\gcd(n,k)=1$ 的最小多项式

定理 3.5.3 (1) $\dim_{\mathbb{Q}}\mathbb{Q}(\zeta_n)=\phi(n)$

(2) 有群同构

$$\begin{aligned}\phi:\mathrm{Aut}(\mathbb{Q}(\zeta_n))&\xrightarrow{\sim} U(\mathbb{Z}_n)\\(\sigma:\zeta_n\mapsto\zeta_n^m)&\longmapsto\overline{m}\end{aligned}$$

证明 (1). 这是定理3.5.2的推论

(2). 同态：设 $\gcd(n,m)=\gcd(n,l)=1,\sigma(\zeta_n)=\zeta_n^m,\tau(\zeta_n)=\zeta_n^l$，则 $\tau\circ\sigma(\zeta_n)=\tau(\zeta_n^m)=\zeta_n^{ml}$，且 $\gcd(n,ml)=1$，故 $\tau\circ\sigma\in\mathrm{Aut}(\mathbb{Q}(\zeta_n))$，且 $\phi(\tau\circ\sigma)=\overline{ml}=\overline{m}\cdot\overline{l}=\phi(\tau)\phi(\sigma)$

双射：由于 $|\mathrm{Aut}(\mathbb{Q}(\zeta_n))|=|U(\mathbb{Z}_m)|=\phi(n)$，所以只需验证单射，因为 $\forall\sigma\in\mathrm{Aut}(\mathbb{Q}(\zeta_n))$ 完全由

$\sigma(\zeta_n)$ 决定，所以

$$\begin{aligned}\sigma \in \mathrm{Ker}(\phi) &\iff \sigma(\zeta_n) = \zeta_n \\ &\iff \sigma = \mathrm{Id}_{\mathbb{Q}(\zeta_n)}\end{aligned}$$

即 $\mathrm{Ker}(\phi) = \{\mathrm{Id}_{\mathbb{Q}(\zeta_n)}\}$，故 ϕ 为单射 □

第四章 群

§4.1 群的定义

定义 4.1.1（群）设 G 为非空集合，$\cdot$ 为二元运算（一般是乘法），称二元组 $(G,\cdot)$ 为群，若

$$\begin{aligned}\cdot : G\times G &\longrightarrow G\\ (a,b) &\longmapsto a\cdot b\end{aligned}$$

满足下面三条公理

(G1) 结合律：$(a\cdot b)\cdot c = a\cdot(b\cdot c)$

(G2) 有幺元：$\exists 1_G\in G, \text{s.t. } \forall a\in G, 1_G\cdot a = a = a\cdot 1_G$

(G3) 有逆元：$\forall a\in G, \exists b\in G, \text{s.t. } a\cdot b = 1_G = b\cdot a$，记 $b = a^{-1}$

特别地，若群 G 称为 Abel 群，则对 $\forall a,b\in G, a\cdot b = b\cdot a$，即满足交换律

评价 为方便表示，也记 $(G,\cdot)$ 为 G；$a\cdot b = ab$

Ex 群 G 中幺元和逆元唯一！

Fact 给定群 $(G,\cdot)$，则

(1) 乘法消去律成立：若 $a\cdot b = a\cdot c$，则 $b = c$；若 $b\cdot a = c\cdot a$，则 $b = c$

(2) $(a^{-1})^{-1} = a$

(3) $(ab)^{-1} = b^{-1}a^{-1}$

Proof : $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}b = 1_G$

(4) $\forall n\in\mathbb{Z}$，定义 a^n 为

$$a^n = \begin{cases}\overbrace{a\cdot a\cdots a\cdot a}^{n\text{个}}, & n>0\\ 1, & n=0\\ (a^{-1})^{-n}, & n<0\end{cases}$$

Ex 验证 $a^{m+n} = a^m\cdot a^n, \forall m,n\in\mathbb{Z}$

约定：我们约定加法群 $(A,+)$ 为 Abel 群，二元运算写为 $+$，它满足

(A1) 结合律：$\forall a,b,c\in A, (a+b)+c = a+(b+c)$

(A2) 有零元：$\exists 0_A\in A, \forall a\in A, a+0_A = a = 0_A+a$

(A3) 有负元：$\forall a\in A, \exists b\in A, \text{s.t. } a+b = 0_A = b+a$，且此时负元唯一，记 $b = -a$

(A4) 交换律：$\forall a,b\in A, a+b = b+a$

例 4.1 $(\mathbb{Z},+),(\mathbb{Q},+)$ 为加法群，$(\mathbb{Q}^\times,\cdot)$ 为乘法群

例 4.2（一般线性群） $\mathrm{GL}_n(\mathbb{C}) = \{A\in \mathrm{M}_n(\mathbb{C})|\det A\neq 0\}$

例 4.3（特殊线性群） $\mathrm{SL}_n(\mathbb{C}) = \{A\in \mathrm{M}_n(\mathbb{C})|\det A = 1\}$

例 4.4（正交群） $\mathrm{O}_n = \{A\in \mathrm{GL}_n(\mathbb{R})|AA^T = I_n\}$

例 4.5（特殊正交群） $\mathrm{SO}_n = \{A\in \mathrm{O}_n|\det A = 1\}$

定义 4.1.2（子群）非空集合 $H \subset G$ 称为 G 的子群，若
(1) $1_G \in H$
(2) 乘法封闭：$\forall a, b \in H, a \cdot b \in H$
(3) 取逆封闭：$\forall a \in H, a^{-1} \in H$
记作 $H \leq G$，特别地 $(H, \cdot)$ 也为群

推论 4.1.1（子群的等价定义）

$$H \leq G \iff \forall a, b \in H, ab^{-1} \in H$$

评价 每个群 G 都有平凡子群 $\{1_G\}$ 和 G

例 4.6 $\mathrm{O}_n \leq \mathrm{GL}_n(\mathbb{R}) \leq \mathrm{GL}_n(\mathbb{C})$

例 4.7 $\mathrm{GL}_1(\mathbb{C}) = \mathbb{C}^\times$，它是 Abel 群，幺元是 1

例 4.8 给定含幺交换环 R，三个与 R 相关的群如下：
(1) 加法群：$(R, +)$
(2) 单位群：$U(R) \overset{\text{def}}{=} \{u \in R | u\text{可逆}\}$，$R$ 为交换环知，$U(R)$ 是 Abel 群
(3) 自同构群：$\mathrm{Aut}(R) = \{\theta : R \xrightarrow{\sim} R : \theta\text{是环自同构}\}$，它的幺元是 Id_R，乘法为映射的复合，如 $f \circ g$，且 $\forall f \in \mathrm{Aut}(R), f^{-1}$ 就是 f 的逆映射

例 4.9 $\forall n \geq 2, \mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$
(1) 加法群：$(\mathbb{Z}_n, +)$
(2) 单位群：$U(\mathbb{Z}_n) \overset{\text{def}}{=} \{\overline{m} | \gcd(m, n) = 1\}$，$|U(\mathbb{Z}_n)| = \phi(n)$
(3) 自同构群：$\mathrm{Aut}(\mathbb{Z}_n) = \{\mathrm{Id}_{\mathbb{Z}_n}\}$，平凡群

例 4.10 给定域扩张 K/k，它的自同构群

$$\mathrm{Aut}(K/k) = \{\sigma \in \mathrm{Aut}(K) | \sigma(\lambda) = \lambda, \forall \lambda \in k\} \leq \mathrm{Aut}(K)$$

定义 4.1.3（正交对称群）$\mathcal{P} \subseteq \mathbb{R}^n$，$\mathcal{P}$ 的正交对称群

$$\Sigma(\mathcal{P}) = \{g \in \mathrm{O}_n | g(\mathcal{P}) = \mathcal{P}\}$$

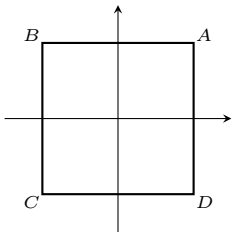
这里 $g(\mathcal{P}) = \mathcal{P}$ 的意思为：①.$\forall v \in \mathcal{P}, g(v) \in \mathcal{P}$；②.$\forall v \in \mathcal{P}, \exists u \in \mathcal{P}, \text{s.t. } v = g(u)$
$\forall g \in \Sigma(\mathcal{P})$，称 g 为 $\mathcal{P}$ 的一个**正交对称**

例 4.11 $n = 2$ 时，考虑圆心位于原点的圆周 $S^1 \subseteq \mathbb{R}^2$，则任意一个正交变换都是圆周 S^1 的正交对称，即

$$\Sigma(S^1) = \mathrm{O}_2$$

例 4.12 $n = 2$ 时，考虑中心位于原点的正方形

$$\Sigma(\square) = \{g \in \mathrm{O}_2 | g(\square) = \square\}$$



如图，考虑正方形的四个顶点组成的集合 $V=\{A,B,C,D\}\subseteq\square,\forall g\in\Sigma(\square)$

$$\begin{cases}A\in V\iff|\overline{OA}|=\sqrt{2}\\|\overline{Og(A)}|=|\overline{OA}|=\sqrt{2}\end{cases}\Longrightarrow g(A)\in V$$

对 B,C,D 同理，因此 $\forall g\in\Sigma(\square),g(V)=V$，故 g 只能是旋转或者对称，若为旋转，则只能旋转 $0°,90°,180°,270°$；若为对称，则 $\overline{Ag(A)}$ 的中垂线为对称轴，若 $A=g(A)$，即 A 在对称轴上，此时一定有 C 在对称轴上。综上对称共有四种，对称轴为 $x=0,y=0,y=x,y=-x$

Ex 写出 $\Sigma(\square)$ 的 8 个矩阵

例 4.13 设 X 是一个抽象集合，称 σ 是 X 上的置换是指 X 到自身的双射

$$\sigma:X\xrightarrow{1:1}X$$

记集合 X 的抽象对称群 (Symmatric group) 为

$$S(X)=\{\sigma:\sigma是X上的置换\}$$

评价 $S(G)$ 有时过大，无法提供较多信息

例 4.14 $\mathrm{Aut}(R)\leq S(R)$，因此在同构意义下有 $\mathrm{GL}_n(\mathbb{C})\leq S(\mathbb{C}^n)$

定理 4.1.1（Cayley, 1878）任何群“本质上”都是某个对称群 $S(X)$ 的子群，实际上对任意群 G，G 与 $S(G)$ 的某个子群同构

定理 4.1.2（Lagrange, 1770）对任意有限群 G，若 $H\leq G$，则

$$|H|\ \big|\ |G|$$

评价 类比：考虑域扩张塔 $k\subseteq E\subseteq K$，则 $\dim_k E\mid\dim_k K$

证明 设 $H\leq G$，对 $\forall a\in G$，定义右陪集

$$Ha\overset{\mathrm{def}}{=}\{ha|h\in H\}\subseteq G$$

Claim: $Ha=Hb\iff ab^{-1}\in H$

Proof Of Claim : ($\Longrightarrow$) 因为 $a = ea \in Ha = Hb$，则 $\exists h \in H, \text{s.t. } a = hb$，所以 $ab^{-1} = h \in H$

($\Longleftarrow$) : 若 $ab^{-1} \in H$，则 $ba^{-1} \in H$，所以 $\forall h \in H, \exists h', h'' \in H, \text{s.t. } h = h' \cdot ab^{-1}, h = h''ba^{-1}$，故

$$\begin{cases} hb = h'ab^{-1}b = h'a \in Ha \Longrightarrow Hb \subseteq Ha \\ ha = h''ba^{-1}a = h''b \in Hb \Longrightarrow Ha \subseteq Hb \end{cases}$$

即 $Ha = Hb$

定义 G 上的关系 $a \approx b \iff Ha = Hb$，由断言知它是一个等价关系，且 a 的关于 $\approx$ 的等价类为 Ha，因此我们得到了 G 的一个分拆

$$G = \bigsqcup_{i \in I} Ha_i$$

其中 $\{a_i\}_{i \in I}$ 为 G 关于 H 的**右陪集完全代表元系**

Key Fact : $|Ha| = |H|$，这是因为

$$H \xrightarrow{1:1} Ha$$
$$h \longmapsto ha$$

由 $|G| < +\infty$ 知 $|I| < +\infty$，故

$$|G| = \sum_{i \in I} |Ha_i| = |H| \cdot |I|$$

□

评价

(1) Lagrange 定理强烈依赖于群的可逆性，即群中任意元素均可逆！考察含幺半群 $(\mathbb{Z}_8, \cdot)$，它有含幺子半群

$$\{\overline{0}, \overline{1}, \overline{3}\}$$

但是 $3 \nmid 8$

(2) 定义 $|I| = [G : H]$ 为 H 的指数，即右陪集的个数，由证明过程我们有

$$|G| = |H| \cdot [G : H]$$

(3) 类似地可以定义左陪集 $aH = \{ah | h \in H\}$，定义等价关系

$$a \approx b \iff aH = bH \iff b^{-1}a \in H$$

也可以证明 Lagrange 定理，从而左陪集的个数与右陪集的个数，即为 $[G : H]$

Ex 若 $G = \bigsqcup_{i \in I} Ha_i$，证明 $G = \bigsqcup_{i \in I} a_i^{-1} H$

例 4.15 考察 $G = \mathrm{GL}_2(\mathbb{F}_2) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in \mathbb{F}_2, \overline{ad - bc} \neq \overline{0} \right\}$

先考虑第一列，由可逆知 (a, c) 的可能取值为 $(1, 0), (0, 1), (1, 1)$，固定第一列后，第二列不能等于第

一列或 $(0,0)$，因此只有两种可能，故 $|G|=3\times 2=6$，具体如下

$$G=\left\{\begin{pmatrix}\overline{1}&\overline{0}\\ \overline{0}&\overline{1}\end{pmatrix},\begin{pmatrix}\overline{1}&\overline{1}\\ \overline{0}&\overline{1}\end{pmatrix},\begin{pmatrix}\overline{0}&\overline{1}\\ \overline{1}&\overline{0}\end{pmatrix},\begin{pmatrix}\overline{0}&\overline{1}\\ \overline{1}&\overline{1}\end{pmatrix},\begin{pmatrix}\overline{1}&\overline{1}\\ \overline{1}&\overline{0}\end{pmatrix},\begin{pmatrix}\overline{1}&\overline{0}\\ \overline{1}&\overline{1}\end{pmatrix}\right\}$$

我们有观察

(1) 幺元为 $\begin{pmatrix}\overline{1}&\overline{0}\\ \overline{0}&\overline{1}\end{pmatrix}=1_G$

(2) 记 $a=\begin{pmatrix}\overline{1}&\overline{1}\\ \overline{0}&\overline{1}\end{pmatrix}$，则 $a^2=\begin{pmatrix}\overline{1}&\overline{0}\\ \overline{0}&\overline{1}\end{pmatrix}=1_G$

(3) 子群 $H=\{1,a\}\leq G$，记 $b=\begin{pmatrix}\overline{0}&\overline{1}\\ \overline{1}&\overline{1}\end{pmatrix},c=\begin{pmatrix}\overline{0}&\overline{1}\\ \overline{1}&\overline{0}\end{pmatrix}$，则

$$G=H\sqcup Hb\sqcup Hc$$

其中

$$Hb=\{b,ab\}=\left\{\begin{pmatrix}\overline{0}&\overline{1}\\ \overline{1}&\overline{1}\end{pmatrix},\begin{pmatrix}\overline{1}&\overline{0}\\ \overline{1}&\overline{1}\end{pmatrix}\right\},\quad Hc=\{c,ac\}=\left\{\begin{pmatrix}\overline{0}&\overline{1}\\ \overline{1}&\overline{0}\end{pmatrix},\begin{pmatrix}\overline{1}&\overline{1}\\ \overline{1}&\overline{0}\end{pmatrix}\right\}$$

但是 $bH\neq Hb$，经计算可得 $ba=c$，但是由 Ex 知

$$G=H\sqcup b^{-1}H\sqcup c^{-1}H$$

定义 4.1.4（阶）设 $a\in G$，定义 a 的阶 (order) 为最小的正整数 $d,\text{s.t. }a^d=1_G$，记作 $d=\mathrm{Ord}(a)$；若为加法群，则定义 a 的阶为最小的正整数 $d,\text{s.t. }da=0_G$

Fact 若 $|G|<+\infty$，则 $\forall a\in G,\mathrm{Ord}(a)<+\infty$

证明 考虑 G 中的无穷序列

$$1,a,a^2,\cdots,a^n,\cdots$$

由 $|G|<+\infty$ 知，一定存在 $i>j,\text{s.t. }a^i=a^j$，所以 $a^{i-j}=1$，故 $\{d>0|a^d=1\}$ 非空，取它的最小元 d

Claim: $d=\mathrm{Ord}(a)$ □

推论 4.1.2 设 $|G|<+\infty,a\in G$，则

$$\mathrm{Ord}(a)\mid |G|$$

证明 $H=\{1,a,\cdots,a^{d-1}\}$ 两两不同，不难验证 $H\leq G,|H|=d$，由 Lagrange 定理知，$d\mid |G|$ □

例 4.16 设 p 为素数，$\mathbb{F}_p^\times=\{\overline{1},\cdots,\overline{p-1}\}$ 是单位群，对 $\forall a\in\mathbb{F}_p^\times,a^{p-1}=\overline{1}$，即 $a^p=a$，故可将费马小定理视为 Lagrange 定理的推论

例 4.17 设 E 是有限域，$E=|p|^n$，则 $|E^\times|=p^n-1$，对 $\forall a\in E^\times,a^{p^n-1}=1_E$，即 $a^{p^n}=a$

例 4.18（阶表）考虑 $G=U(\mathbb{Z}_8)=\{\overline{1},\overline{3},\overline{5},\overline{7}\}$，它的阶表为

	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$
Ord	1	2	2	2

例 4.19 若 $G=(\mathbb{Z}_4,+)=\{\overline{0},\overline{1},\overline{2},\overline{3}\}$，它的阶表为

	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
Ord	1	4	2	4

因此 $(\mathbb{Z}_4,+)$ 与 $(U(\mathbb{Z}_8),\cdot)$ 显然不同构!

定义 4.1.5（群同态、群同构）设 G,H 为群，映射 $f:G\to H$ 称为群同态，若

$$f(ab)=f(a)f(b),\quad \forall a,b\in G$$

若 f 还是双射，则称 f 为群同构

命题 4.1.1 设 $f:G\to H$ 是群同态

(1) $f(1_G)=1_H$

Proof: $f(1_G\cdot 1_G)=f(1_G)f(1_G)$，由 H 中的消去律得 $f(1_G)=1_H$

(2) $f(a^{-1})=f(a)^{-1},\forall a\in G$

Ex $f:G\to H$ 为群同态，G,H 为有限群，$a\in G$，则 $\mathrm{Ord}(f(a))\mid\mathrm{Ord}(a)$；若 f 为同构，则 $\mathrm{Ord}(a)=\mathrm{Ord}(f(a))$，因此同构的群阶表相同（对应元素的阶相同）

例 4.20 $U(\mathbb{Z}_8)$ 不同构于 $(\mathbb{Z}_4,+)$

Ex 考察求逆映射

$$\begin{aligned}(-)^{-1}:G&\longrightarrow G\\ g&\longmapsto g^{-1}\end{aligned}$$

则 $(-)^{-1}$ 是群同态 $\iff$ G 是 *Abel* 群

Ex 定义 G 的反群 $G^{\mathrm{op}}=\{a^{\mathrm{op}}|a\in G\}$，乘法定义为 $a^{\mathrm{op}}b^{\mathrm{op}}=(ba)^{\mathrm{op}}$，求证 G 同构于 G^{op}

例 4.21 行列式映射

$$\begin{aligned}\det:\mathrm{GL}_n(\mathbb{C})&\longrightarrow\mathbb{C}^\times\\ A&\longmapsto\det(A)\end{aligned}$$

是群同态

Ex $\forall n\geq 2,\mu_n=\{z\in\mathbb{C}|z^n=1\}\leq\mathbb{C}^\times$，证明 $(\mu_n,\cdot)$ 同构于 $(\mathbb{Z}_n,+)$

定义 4.1.6（群的直积）设 G,H 是群，定义

$$G\times H=\{(g,h)|g\in G,h\in H\}$$

为 G 与 H 的直积，它的幺元为 $(1_G, 1_H)$，乘法定义为 $(g,h)\cdot(g',h')=(gg',hh')$

评价

(1) 典范单同态

$$G \longrightarrow G\times H$$
$$g \longmapsto (g,1_H)$$

(2) 投影映射（满射）

$$G\times H \xrightarrow{Pr} G$$
$$(g,h) \longmapsto g$$

(3) 元素分解：$\forall (g,h)\in G\times H, (g,h)=(g,1_H)\cdot(1_G\cdot h)$

(4) $\mathrm{Ord}(g,h)=\mathrm{lcm}(\mathrm{Ord}(g),\mathrm{Ord}(h))$

Ex 回忆 $\mu_2=\{1,-1\}$，记 $\mu_2\times\mu_2=V_4$，称为 *Klein* 四群，证明 $V_4\simeq U(\mathbb{Z}_8)$

§4.2 循环群

定义 4.2.1（生成子群）设 G 是群，给定子集 $X\subseteq G$，记

$$\begin{aligned}(X) &= \text{包含}X\text{的最小子群}\\ &= \{x_1x_2\cdots x_n | \forall i, x_i\in X \text{或} x_i^{-1}\in X\}\end{aligned}$$

称 (X) 为由 X 生成的最小子群，特别地若 $X=\{a\}$，则

$$(a)=\{\cdots,a^{-2},a^{-1},1,a,a^2,\cdots\}$$

定义 4.2.2（循环群）称 G 为循环群 (Cyclicgroup)，若 $\exists a\in G, \text{s.t. } (a)=G$，此时 a 为 G 的生成元；循环群一定是 Abel 群！

例 4.22

- $\mu_n=\left(e^{\frac{2\pi i}{n}}\right)$ 是循环群
- $(\mathbb{Z},+)$ 是循环群，它可以由 1 或 -1 生成
- $(\mathbb{Z}_n,+)$ 是循环群

命题 4.2.1 设 G 为循环群，则 G 同构于 $(\mathbb{Z},+)$ 或 $(\mathbb{Z}_n,+)$

证明 取 G 的一个生成元 a，则

$$G=\{a^n | n\in\mathbb{Z}\}$$

Case 1. $\mathrm{Ord}(a)=+\infty$

则 $a^m\neq a^n, \forall m\neq n$（否则 $a^{n-m}=1_G$，矛盾！），因此我们有群同构

$$(\mathbb{Z},+) \xrightarrow{\sim} (G,\cdot)$$
$$n \longmapsto a^n$$

Case 2. $\mathrm{Ord}(a)=n<+\infty$

则 $G=(a)=\{1,a,\cdots,a^{n-1}\}$，因此我们有群同构

$$\begin{aligned}(\mathbb{Z}_n,+)&\longrightarrow(G,\cdot)\\ \overline{n}&\longmapsto a^n\end{aligned}$$

□

评价 n 阶循环群 $\simeq(\mathbb{Z}_n,+)\simeq\mu_n$

命题 4.2.2 设 $G=(a)$ 为循环群，则

(1) 若 $|G|=+\infty$，则

- G 恰有两个生成元 a,a^{-1}
- G 的子群如下：$\{1_G\},\left(a^d\right),d\geq 1$，且 $\left(a^d\right)\simeq G$

(2) 若 $|G|=n<+\infty$，则

- G 恰有 $\phi(n)$ 个生成元 $\{a^k|1\leq k\leq n-1,\gcd(k,n)=1\}$
- 对 $\forall d\mid n,\exists! d$ 阶子群 $H_d=\left(a^{\frac{n}{d}}\right)\leq G$，因此我们有一一对应

$$\begin{aligned}\{G\text{的子群}\}&\overset{1:1}{\longleftrightarrow}\{d:d\mid n,1\leq d\leq n\}\\ H_d&\longmapsto d\end{aligned}$$

评价 将 G 分别同构到 $(\mathbb{Z},+),(\mathbb{Z}_n,+)$，将生成元打到 1，考察 $(\mathbb{Z},+),(\mathbb{Z}_n,+)$ 的子群即可证明

例 4.23 无限循环群 $(\mathbb{Z},+)\simeq\left\{\begin{pmatrix}1&n\\0&1\end{pmatrix}\middle|n\in\mathbb{Z}\right\}\leq\mathrm{SL}_2(\mathbb{R})$

Fact 设 $G=(a)$ 为有限循环群，$|G|=n$，则

(1) $\mathrm{Ord}(a^l)=\frac{n}{\gcd(n,l)}$

(2) 若 $x\in G,\mathrm{Ord}(x)=d$，则 $|\{x\in G|\mathrm{Ord}(x)=d\}|=\phi(d)$，即 d 阶元的个数为 $\phi(d)$

Proof：考察 $\gcd(k,d)=1$，若 a 为 d 阶元，则 a^k 也为 d 阶元

(3) 按阶数对 G 进行剖分 $n=\sum\limits_{d\mid n}\phi(d)$

$$|G|=\sum_{d\mid n}|\{x\in G|\mathrm{Ord}(x)=d\}|$$

(4) G 有唯一 d 阶子群 $H_d=\{1,a^{\frac{n}{d}},a^{\frac{2n}{d}},\cdots\}$

Fact 若 $|G|=n<+\infty$，则 G 为循环群 $\iff$ G 有 n 阶元

证明 $(\Longrightarrow)$：由定义显然

$(\Longleftarrow)$：设 $a\in G,\mathrm{Ord}(a)=n$，则

$$(a)=\{1,a,\cdots,a^{n-1}\}\leq G$$

且二者大小相同，故 $G=(a)$ □

推论 4.2.1 设 p 为素数，则 p 阶群 $\simeq \mu_p$

证明 对 $1_G \neq a \in G$，因为 $1<\mathrm{Ord}(a) \mid |G|=p$，所以 $\mathrm{Ord}(a)=G$，即 $G=(a)$ □

定理 4.2.1 设 $|G|=n<+\infty$，则

$$G\text{是循环群} \iff \forall d \mid n,\ \text{至多存在一个}d\text{阶子群}$$

证明 $(\Longrightarrow)$：上面已经证明

$(\Longleftarrow)$：对 $\forall d \mid n$，定义

$$S_d=\{g\in G|\mathrm{Ord}(g)=d\}$$

则 $G=\bigsqcup\limits_{d|n} S_d$

Claim: $S_d\neq\varnothing, \forall d\mid n$

Proof Of Claim : $\forall d\mid n$，若 $S_d\neq\varnothing$，则 $\forall g\in S_d$，则 $H_d=(g)\leq G$ 为 G 的 d 阶子群，且由公式

$$\mathrm{Ord}(g^k)=\frac{d}{\gcd(k,d)}$$

知，恰有 $\phi(d)$ 个 k 满足 $\gcd(k,d)=1$，故这 $\phi(d)$ 个 g^k 均在 S_d 中，由至多存在一个 d 阶子群知 $S_d\subseteq H_d$，所以

$$|G|=\left|\bigsqcup_{d|n} S_d\right|=\sum_{d|n}|S_d|\leq\sum_{d|n}\phi(d)=n=|G|$$

□

定理 4.2.2 设 k 为域，$G\leq k^\times$，若 $|G|<+\infty$，则 G 是循环群；特别地，若 $|G|=n$，G 的生成元为 k 中的 n 次本原单位根

证明 设 $|G|=n$，对 $\forall d\mid n, \exists H_d\leq n$ 为 d 阶子群，取 H 的生成元 g，则 $g^d=1_G=1_k$，所以

$$H\subseteq \mathrm{Root}_k(x^d-1)$$

二者大小均为 d，故 $H=\mathrm{Root}_k(x^d-1)$ 至多唯一！ □

例 4.24 $\mathbb{C}^\times$ 的有限子群恰为 $\mu_n, n\geq 1$，但 $\mathbb{C}^\times$ 不是循环群（$\mathbb{C}$ 甚至都不可数）！

Ex 证明 $\mathbb{Q}^\times$ 不是循环群

推论 4.2.2 设 E 是有限域，则 $E^\times$ 是 p^n-1 阶循环群，因此 $E/\mathbb{F}_p$ 是单扩张！

§4.3 正规子群

引入：考虑群同态 $f:G\to H$，我们有

$$\begin{cases} f(ab)=f(a)f(b),\forall a,b\in G \\ f(1_G)=1_H \\ f(a^{-1})=f(a)^{-1} \end{cases}$$

考虑 f 的像集 $\mathrm{Im}f=f(G)\leq H$，类似环同态基本定理，定义 G 上的等价关系

$$\begin{aligned} a\overset{f}{\sim}b &\iff f(a)=f(b)\text{ in }H \\ &\iff f(ab^{-1})=1_H \\ &\iff f(b^{-1}a)=1_H \end{aligned}$$

评价 一般情况 $ab^{-1}\neq b^{-1}a$，但它们“相似”：

$$ab^{-1}=a(b^{-1}a)a^{-1}$$

定义 4.3.1（群同态的核）设 $f:G\to H$ 是群同态，定义群同态的核

$$N\overset{\text{def}}{=}\mathrm{Ker}(f)=\{a\in G|f(a)=1_H\}\leq G$$

评价

(1) $\forall a\in N,f(a^{-1})=f(a)^{-1}=1_H^{-1}=1_H$，故 $a^{-1}\in N$

(2) 回忆 Lagrange 定理的证明

$$\begin{aligned} f(a)=f(b) &\iff ab^{-1}\in N\iff Na=Nb \\ &\iff b^{-1}a\in N\iff aN=bN \end{aligned}$$

引理 4.3.1 $\forall a\in G,N=\mathrm{Ker}(f)$，则 $aN=Na$

证明 因为

$$b\in aN\iff b^{-1}a\in N\iff ab^{-1}\in N\iff b\in Na$$

□

定义 4.3.2（正规子群） $N\leq G$ 称为正规子群，若 $\forall a\in G,\boxed{aN=Na}$，记作 $N\trianglelefteq G$

Fact $\forall f:G\to H,\mathrm{Ker}(f)\trianglelefteq G$

例 4.25 设 G 是 *Abel* 群，则任意 G 的子群均为正规子群

例 4.26 $\left\{\begin{pmatrix}\overline{1}&\overline{0}\\\overline{0}&\overline{1}\end{pmatrix},\begin{pmatrix}\overline{1}&\overline{1}\\\overline{0}&\overline{1}\end{pmatrix}\right\}\leq \mathrm{GL}_2(\mathbb{F}_2)$ 不正规

Ex 证明群 G 的中心 $Z(G)$ 是正规子群，其中

$$Z(G)=\{g\in G|gh=hg,\forall h\in G\}$$

Fact 对 $\forall U\leq G, a\in G$，U 的共轭是 G 的正规子群

$$aUa^{-1}=\{aha^{-1}|h\in U\}\trianglelefteq G$$

且我们有群同构 $U\simeq aUa^{-1}$，但它们做为集合一般不相等

Fact 设 $N\leq G$，则

$$N\trianglelefteq G\iff \forall a\in G, N=aNa^{-1}$$

评价 “正规”性可以理解为“共轭不变性”

例 4.27 $\mathrm{GL}_2(\mathbb{F}_2)$ 有非平凡正规子群

$$\left\{\begin{pmatrix}\overline{1}&\overline{0}\\\overline{0}&\overline{1}\end{pmatrix},\begin{pmatrix}\overline{0}&\overline{1}\\\overline{1}&\overline{1}\end{pmatrix},\begin{pmatrix}\overline{1}&\overline{1}\\\overline{1}&\overline{0}\end{pmatrix}\right\}$$

因为

$$\begin{pmatrix}\overline{0}&\overline{1}\\\overline{1}&\overline{1}\end{pmatrix}^3=\begin{pmatrix}\overline{0}&\overline{1}\\\overline{1}&\overline{1}\end{pmatrix}\begin{pmatrix}\overline{0}&\overline{1}\\\overline{1}&\overline{1}\end{pmatrix}\begin{pmatrix}\overline{0}&\overline{1}\\\overline{1}&\overline{1}\end{pmatrix}=\begin{pmatrix}\overline{1}&\overline{1}\\\overline{1}&\overline{0}\end{pmatrix}\begin{pmatrix}\overline{0}&\overline{1}\\\overline{1}&\overline{1}\end{pmatrix}=\begin{pmatrix}\overline{1}&\overline{0}\\\overline{0}&\overline{1}\end{pmatrix}$$

评价 数学忌崇拜！人人平等！

Ex 设 $N\leq G$，若 $[G:N]=2$，证明 $N\trianglelefteq G$

例 4.28 考虑 $\det:\mathrm{GL}_n(\mathbb{C})\to\mathbb{C}^\times$，它的核 $\mathrm{SL}_n\trianglelefteq GL_n(\mathbb{C})$

例 4.29 考虑 $\mathrm{M}_n(\mathbb{C})$ 中对角元均为 1 的上三角阵全体 $U_n(\mathbb{C})\leq \mathrm{GL}_n(\mathbb{C})$，它不是正规子群！

定义 4.3.3（商群）设 $N\trianglelefteq G$，定义 N 在 G 上的商群

$$G/N=\{aN|a\in G\}$$

它的大小为 $|G/N|=[G:N]$，记 $aN=\overline{a}$，则 $\overline{a}=\overline{b}\iff ab^{-1}\in N\iff b^{-1}a\in N$

引理 4.3.2（陪集上乘法的良定性）我们希望在商群上定义乘法

$$\overline{a}\cdot\overline{b}=\overline{ab}$$

验证它的良定性；设 $\overline{a}=\overline{a}',\overline{b}=\overline{b}'$，是否有 $\overline{ab}=\overline{a'b'}$？事实上

$$\begin{aligned}(a'b')^{-1}ab&=b'^{-1}a'^{-1}ab\\&=b'^{-1}bx,x\in N\\&=(b'b)x\in N\end{aligned}$$

第二行是因为 $a'^{-1}a\in N$，则 $a'^{-1}ab\in Nb=bN$，可设它为 $bx,x\in N$

Fact $\overline{1}_{G/N}=\overline{1},\overline{a}^{-1}=\overline{a^{-1}}$

Fact 我们有典范（满）同态

$$\begin{aligned}\mathrm{can}:G&\longrightarrow G/N\\a&\longmapsto\overline{a}=aN\end{aligned}$$

其中 $\mathrm{Ker}(\mathrm{can})=N$

定理 4.3.1（群同态基本定理）设 $f:G\to H$ 是群同态，则 $\mathrm{Im}(f)\le H,\mathrm{Ker}(f)\trianglelefteq H$，且 f 诱导唯一群同构

$$\begin{aligned}\overline{f}:G/\mathrm{Ker}(f)&\xrightarrow{\sim}\mathrm{Im}(f)\\\overline{a}&\longmapsto f(a)\end{aligned}$$

即下面的图交换

$$\begin{array}{ccc}G & \xrightarrow{\quad f\quad} & H\\ {\scriptstyle\mathrm{can}}\downarrow & & \uparrow{\scriptstyle\mathrm{inc}}\\ G/\mathrm{Ker}(f) & \xrightarrow[\overline{f}]{\cdots\cdots\cdots} & \mathrm{Im}(f)\end{array}$$

证明 因为 $a\mathrm{Ker}(f)=b\mathrm{Ker}(f)\iff a\overset{f}{\sim}b$ □

评价

- f 是单射 $\iff\mathrm{Ker}(f)=\{1_G\}$，此时有群同构 $G\xrightarrow{\sim}\mathrm{Im}(f)\le H$
- f 是满射 $\iff\mathrm{Im}(f)=H$，此时有群同构 $G/\mathrm{Ker}(f)\xrightarrow{\sim}H$

定理 4.3.2（对应定理）设 $N\trianglelefteq G$，则

$$\begin{aligned}\{K|N\le K\le G\}&\xrightarrow{1:1}\{G/N\text{的子群}\}\\K&\longmapsto K/N\\\{a\in G|\overline{a}\in L\}&\longmapsfrom L\end{aligned}$$

此时 $K\trianglelefteq G\iff(K/N)\trianglelefteq(G/N)$，且有群同构

$$(G/N)/(K/N)\xrightarrow{\sim}G/K$$

证明 设 $L \leq G/N$，验证上面给出的关系是互逆的；特别地

$$K \trianglelefteq G \Longrightarrow \overline{a}(K/N)\overline{a}^{-1} = (aKa^{-1})/N = K/N$$

若 $N \trianglelefteq K \trianglelefteq G$，则有群同态

$$\begin{aligned} \sigma : (G/N) &\longrightarrow (G/K) \\ aN &\longmapsto aK \end{aligned}$$

$\mathrm{Ker}(\sigma) = \{aN | aK = 1_{G/K}\} = \{aN | a \in K\} = K/N \trianglelefteq G/N$ □

定理 4.3.3（第二群同构定理）设 $N \trianglelefteq G, H \leq G$，则
(1) $NH = HN \ \therefore N \leq NH \leq G$
(2) $(N \cap H) \trianglelefteq H$，且有群同构 $H/(N \cap H) \xrightarrow{\sim} (NH)/H$

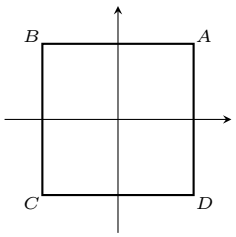
证明 只证明 (2)，因为

$$\begin{aligned} H \overset{\text{inc}}{\hookrightarrow} G &\overset{\text{can}}{\rightrightarrows} G/N \\ h &\mapsto \ h \ \mapsto \overline{h} \end{aligned}$$

它的像 $(NH)/N = \{\overline{hn} | hn \in NH\}$，核为 $\{h \in H | \overline{h} = \overline{1}\} = \{h \in H | h \in N\} = N \cap H$，由群同态基本定理即证 □

Ex P17 5, 13 P20 3, 10 P25 7, 10

例 4.30 回忆：中心位于原点的正方形



它的正交对称群为 $\Sigma(\square) = \{g \in \mathrm{O}_2 | g(\square) = \square\} \leq \mathrm{O}_2$，记它的顶点集合 $V = \{A, B, C, D\}$，设 $S(V) = \{\sigma : V \to V\}$ 为 V 的（抽象）对称群，则 $|S(V)| = 4! = 24$，我们有群同态

$$\begin{aligned} \phi : \Sigma(\square) &\longrightarrow S(V) \\ g &\longmapsto (g|_V : V \xrightarrow{\sim} V) \end{aligned}$$

***Claim*:** ϕ 是单射，故 $\Sigma(\square) = \mathrm{Im}(\phi)$
Proof Of Claim : 只需证明 $\mathrm{Ker}(\phi)$ 是平凡子群

$$\begin{aligned} \mathrm{Ker}(\phi) &= \{g \in \Sigma(\square) : g|_V = \mathrm{Id}_V\} \\ &= \{g \in \Sigma(\square) : g(\overrightarrow{OM}) = \overrightarrow{OM}, M \in V\} \\ &= \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} \end{aligned}$$

例 4.31 设 $f(x)=x^3-2\in\mathbb{Q}[x]$，$E=\mathbb{Q}(\sqrt[3]{2},\sqrt[3]{2}\omega,\sqrt[3]{2}\omega^2)=\mathbb{Q}(\sqrt[3]{2},\omega)$ 为 $f(x)$ 的分裂域，则

$$|\mathrm{Aut}(E)|=|\mathrm{Aut}(E/\mathbb{Q})|=\dim_{\mathbb{Q}}E=6$$

记 $X=\mathrm{Root}_E(x^3-2)=\{\sqrt[3]{2},\sqrt[3]{2}\omega,\sqrt[3]{2}\omega^2\}\overset{\text{def}}{=}\{a,b,c\}$，设 $S(X)=\{\sigma:X\xrightarrow{\sim}X\}$ 为 X 的抽象对称群，则 $|S(X)|=6$

Claim: 有群同态

$$\begin{aligned}\phi:\mathrm{Aut}(E):&\longrightarrow S(X)\\ \sigma&\longmapsto(\sigma|_X:X\xrightarrow{\sim}X)\end{aligned}$$

Key Claim ϕ 是单射

Proof Of Claim : 因为

$$\begin{aligned}\mathrm{Ker}(\phi)&=\{\sigma\in\mathrm{Aut}(E):\sigma|_X=\mathrm{Id}_X\}\\&=\{\sigma\in\mathrm{Aut}(E):\sigma(x)=x,x=a,b,c\}\\&=\{\mathrm{Id}_E\}\end{aligned}$$

所以 ϕ 是群同构！即 $\mathrm{Aut}(E)\simeq S(X)\simeq S_3$

§4.4 对称群

定义 4.4.1（对称群）设 X 是集合，S 上的双射全体记为

$$S(X)=\{\sigma:X\xrightarrow{\sim}X\}$$

称为 X 的抽象对称群；若 $X=\{1,2,\cdots,n\}$，则记 $S(X)=S_n$

Fact 若存在双射 $X\xrightarrow[\sim]{\delta}Y$，则有群同构

$$\begin{aligned}S(X)&\longrightarrow S(Y)\\ \sigma&\longmapsto\delta\sigma\delta^{-1}\end{aligned}$$

推论 4.4.1 设 $|X|=n$，则 $S(X)\simeq S_n$，即 n 阶群在同构意义下唯一。因此为方便表示，我们研究 $X=\{1,2,\cdots,n\}$

Fact $|S_n|=n!$

例 4.32 S_1 为平凡群；$S_2=\{\mathrm{Id},\sigma\}$ 为 Abel 群；若 $n\geq3$，则 S_n 非交换

约定：对于 $\sigma\in S_n,\forall1\leq i\leq n$，我们用

$$\sigma=\begin{pmatrix}1&2&\cdots&n\\ \sigma(1)&\sigma(2)&\cdots&\sigma(n)\end{pmatrix}$$

来表示 σ，其中第一行为定义域，第二行为取值，显然有

$$\sigma^{-1}=\begin{pmatrix}\sigma(1) & \sigma(2) & \cdots & \sigma(n)\\ 1 & 2 & \cdots & n\end{pmatrix}$$

且 $|S_n|=n!$

例 4.33 $|S_3|=3!=6$，设 $\sigma=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\delta=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\tau=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$，则

$$\sigma^{-1}=\begin{pmatrix}2&1&3\\1&2&3\end{pmatrix}=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=\sigma$$

$$\delta^{-1}=\begin{pmatrix}2&3&1\\1&2&3\end{pmatrix}=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\neq\delta$$

***Q*:** 如何求 δ^2?

$\delta\circ\delta(1)=\delta(2)=3,\delta\circ\delta(2)=\delta(3)=1,\delta\circ\delta(3)=\delta(1)=2$，类似地我们发现 $\delta^3=\mathrm{Id}_{S_3}$

***Q*:** 如何求 $\sigma\circ\tau$?

对于每个元素逐一计算即可

$$\sigma\circ\tau=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=\delta$$

Fact 对 $\forall n\geq 3,S_n$ 不是 Abel 群！因为 $\sigma\circ\tau\neq\tau\circ\sigma$

证明 考虑嵌入同态

$$S_n\longrightarrow S_{n+1}$$
$$\sigma\longmapsto\overline{\sigma}$$

其中 $\overline{\sigma}|_{S_n}=\sigma,\overline{\sigma}(n+1)=n+1$，进而在 S_n 中，$\overline{\sigma}\circ\overline{\tau}\neq\overline{\tau}\circ\overline{\sigma}$，其中 σ,τ 是上面 S_3 中不可交换的例子□

定义 4.4.2（轮换）设 $t\geq 2,\{i_1,i_2,\cdots,i_t\}\subseteq\{1,2,\cdots,n\}$，记 $c=(i_1i_2\cdots i_t)\in S_n$，表示

$$c:i_1\mapsto i_2\mapsto\cdots\mapsto i_t\mapsto i_1$$

若 $j\in\{i_1,i_2,\cdots,i_t\}^c\cap\{1,2,\cdots,n\}$，则 $c(j)=j$，称 $c\in S_n$ 为 t-轮换

评价

(1) $\mathrm{Ord}(c)=t,c^t=\mathrm{Id}$

(2) 若 $c=(i_1i_2\cdots i_t)$，则 $c^{-1}=(i_ti_{t-1}\cdots i_1)$

(3) 2-轮换也称**对换**，且 $(ij)=(ji)$，且 $(ij)^2=\mathrm{Id}$，S_n 中对换的个数为 $\frac{n(n-1)}{2}$

(4) 1-轮换是平凡的，可以略去不写

(5) $(i_1i_2i_3)=(i_2i_3i_1)=(i_3i_1i_2)$，对 t-轮换也类似，即同一个轮换有多种表达方式，一般习惯把数字小的放到前面

(6) 同一个 t-轮换有 t 种不同的表达形式，因此 t 轮换共有 $\binom{n}{t}\cdot t!\cdot\frac{1}{t}=\frac{n!}{(n-t)!t}$ 种

例 4.34 $S_2 = \{\mathrm{Id}, (12)\}$

$S_3 = \{\mathrm{Id}, (12), (13), (23), (132), (123)\}$，注意到 $(132)^{-1} = (123)$

并非所有元素都是 t-轮换！在 S_4 中

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (12)(34)$$

其中 $(12)(34)$ 表示 $(12) \circ (34)$，但是一般不写出来

引理 4.4.1 设 $\sigma \in S_n$，给定 t 轮换 $(i_1\ i_2\ \cdots\ i_t)$，则

$$\sigma \circ (i_1 i_2 \cdots i_t) \circ \sigma^{-1} = \big(\sigma(i_1)\sigma(i_2)\cdots\sigma(i_t)\big)$$

证明 因为

$$\sigma \circ (i_1 i_2 \cdots i_t) \circ \sigma^{-1}\big(\sigma(i_r)\big) = \sigma(i_{r+1})$$

□

引理 4.4.2 在 S_n 中，设 σ, τ 是轮换，若 σ, τ 不相交，则 $\sigma \circ \tau = \tau \circ \sigma$

证明 设 $\tau = (i_1 i_2 \cdots i_t)$，根据引理 4.4.1

$$\sigma \circ \tau \circ \sigma^{-1} = \big(\sigma(i_1)\sigma(i_2)\cdots\sigma(i_t)\big) \overset{\text{不相交}}{=\!=} (i_1 i_2 \cdots i_t)$$

□

例 4.35 在 S_3 中，设 $\sigma = (12), \tau = (23)$，则

$$(12)(23)(12)^{-1} = \big(\sigma(2)\sigma(3)\big) = (13)$$

$$(23)(12)(23)^{-1} = \big(\tau(1)\tau(2)\big) = (13)$$

因此在 S_3 中，$\sigma\tau\sigma = \tau\sigma\tau \Longrightarrow (\sigma\tau)^3 = \mathrm{Id}$

命题 4.4.1（轮换的分解）对 $\forall \sigma \in S_n$，存在唯一两两不交的轮换 $c_1, \cdots, c_l$，使得

$$\sigma = c_1 c_2 \cdots c_l$$

证明 设 $\sigma \in S_n$，首先考虑数字 1 所在的轮换，考虑 $\{1, 2, \cdots, n\}$ 上 1 的 σ-轨道

$$\left\{1 \quad \sigma(1) \quad \sigma^2(1) \quad \cdots\right\}$$

Case 1. 若 $\sigma(1) = 1$，则为 (1)

Case 2. 若 $\sigma(1)\neq 1,\sigma^2=1$，则为 $\begin{pmatrix}1 & \sigma(1)\end{pmatrix}$

Case 3. 若 $\sigma(1)\neq 1,\sigma^2(1)\neq 1,\sigma^3(1)=1$，则为 $\begin{pmatrix}1 & \sigma(1) & \sigma^2(1)\end{pmatrix}$

Case 4. $\cdots$

除去 1 所在的轮换中的元素，对其它元素也类似操作即可 □

例 4.36 在 S_7 中，化简 $(456)(567)(761)$ 为轮换的乘积

解 复合映射，从右往左读

$1\mapsto 7\mapsto 5\mapsto 6, 6\mapsto 1$，所以有 (16)

$2\mapsto 2$，所以有 (2)

$3\mapsto 3$，所以有 (3)

$4\mapsto 5, 5\mapsto 6\mapsto 4$，所以有 (45)

$7\mapsto 6\mapsto$，所以有 (7)

因此 $\sigma=(16)(45)$

定义 4.4.3（型）设 $\sigma=c_1\cdots c_n$ 为两两不交的轮换的乘积，其中 i-轮换的个数为 λ_i，则 σ 的型为

$$1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$$

评价 有定义立刻有 $\sum\limits_{i=1}^{n} i\lambda_i=n$

定理 4.4.1 $\sigma,\tau\in S_n$ 共轭 $\iff$ σ,τ 同型

证明 $(\Longrightarrow)$：设 $\sigma=c_1\cdots c_l$ 为两两不交的轮换的乘积，由共轭知 $\exists h\in S_n, \text{s.t. } \tau=h\sigma h^{-1}$，因此

$$\tau=h\sigma h^{-1}=(hc_1h^{-1})(hc_2h^{-1})\cdots(hc_lh^{-1})$$

由引理 4.4.1，$\tau c_1\tau^{-1}$ 和 c_1 是同阶轮换，因此它们同型

$(\Longleftarrow)$：设 σ,τ 同型，设

$$\begin{cases}\sigma=(a_1)\cdots(a_s)\cdots(b_1b_2)\cdots\\ \tau=(a_1')\cdots(a_s')\cdots(b_1'b_2')\cdots\end{cases}$$

考虑 $h\in S_n$ 如下（即将对应的 t-轮换中的元素做对应，注意到我们只是随意将同阶轮换进行排列，故 h 不唯一）

$$\begin{aligned}h:\{1,2,\cdots,n\}&\longrightarrow\{1,2,\cdots,n\}\\ a_j&\longmapsto a_j'\\ b_i&\longmapsto b_i'\end{aligned}$$

不难验证 $\tau=h\sigma h^{-1}$ □

推论 4.4.2 假设 $H\trianglelefteq S_n$，则它一定包含了某一整个共轭类，即所有型相同的元素

例 4.37 S_3, S_4 的共轭类如下

型	1^3	1^12^1	3^1
元素	Id	$(12),(13),(23)$	$(123),(132)$

型	1^4	1^22^1	2^2	1^13^1	4^1
元素	Id	$(12),(13)$ $(14),(23)$ $(24),(34)$	$(12)(34)$ $(13)(24)$ $(14)(23)$	$(123),(132)$ $(124),(142)$ $(134),(143)$ $(234),(243)$	$(1234),(1243)$ $(1324),(1342)$ $(1423),(1432)$

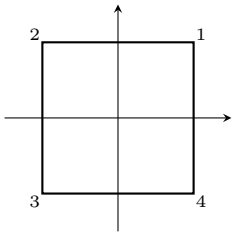
例 4.38 考虑嵌入同态 $S_3 \overset{保4}{\hookrightarrow} S_4$，因为

$$(14)(12)(14)^{-1} = (24) \notin S_3$$

所以 S_3 不是 S_4 的正规子群！

例 4.39 考虑正方形的正交对称群到 S_4 的嵌入同态 $\Sigma(\square) \hookrightarrow S_4$，它的像为（记为 H）

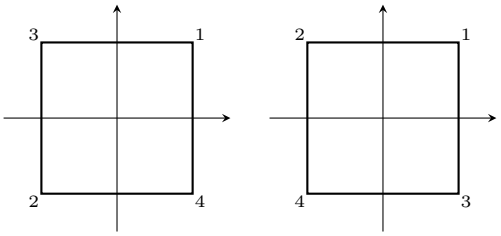
1. 四个旋转：$\mathrm{Id}, (1234), (13)(24), (1432)$
2. 四个对称：$(14)(23), (12)(34), (24), (13)$



Q：在像群 H 中，$(13)(24), (14)(23)$ 是否共轭？

A：不共轭！它们的原像的行列式为 1 和 -1，共轭矩阵的行列式相等，故不共轭！

Ex 若正方形顶点的编号变为



同例 4.39，分别计算 $\Sigma(\square)$ 到 S_4 的嵌入同态的像集 H', H''，并且计算 $H \cap H' \cap H''$

Ex 证明上面的 H 为由 $(13), (1234)$ 生成的子群

Fact S_n 可以由 $(12), (23), \cdots, (n-1, n)$ 生成

证明 Step 1. 我们可以将任意一个 t-轮换写为 $t-1$ 个对换之积

$$(i_1 i_2 \cdots i_t) = (i_{t-1} i_t) \cdots (i_2 i_t)(i_1 i_t)$$

Step 2. 当 $i<j$ 时，$(ij)=(i+1,j)(i,i+1)(i+1,j)^{-1}$，对 $(i+1,j)$ 继续处理，进而第一步中的每个 (i_ji_t) 均可以写为相邻对换之积 □

评价 群表示的角度：在 S_n 中，令 $s_i=(i,i+1),1\le i\le n-1$，则

(1) $s_i^2=\mathrm{Id}$

(2) $s_is_{i+1}s_i=s_{i+1}s_is_{i+1}$

(3) $s_is_j=s_js_i$ as $|j-i|\ge 2$

评价 大家没事干可以挑战一下自己学一下李代数

定义 4.4.4（置换矩阵）给定 $\sigma\in S_n$，我们有线性变换

$$\begin{aligned} P_\sigma:\mathbb{R}^n &\longrightarrow \mathbb{R}^n\\ \boldsymbol{e}_i &\longmapsto \boldsymbol{e}_{\sigma(i)}\end{aligned}$$

而线性变换对应的矩阵（也记为 P_σ）为 $P_\sigma=\begin{pmatrix}\boldsymbol{e}_{\sigma(1)} & \boldsymbol{e}_{\sigma(2)} & \cdots & \boldsymbol{e}_{\sigma(n)}\end{pmatrix}$

定义 4.4.5（奇/偶置换）我们有群同态

$$\begin{aligned}\phi:S_n &\longrightarrow \mathrm{GL}_n(\mathbb{R})\\ \sigma &\longmapsto P_\sigma\end{aligned}$$

它确实是群同态，因为

$$P_\sigma\circ P_\tau(\boldsymbol{e}_i)=P_\sigma(\boldsymbol{e}_{\tau(i)})=P_{\sigma(\tau(i))}=P_{\sigma\tau}(\boldsymbol{e}_i)$$

再将它与行列式同态复合，记 $\det\circ\phi=\mathrm{sgn}$，则有群同态

$$\begin{aligned}\mathrm{sgn}:S_n &\longrightarrow \{-1,1\}\\ \sigma &\longmapsto \det(P_\sigma)\end{aligned}$$

若 $\mathrm{sgn}(\sigma)=1$，则称 σ 为偶置换；若 $\mathrm{sgn}(\sigma)=-1$，则称 σ 为奇置换，定义

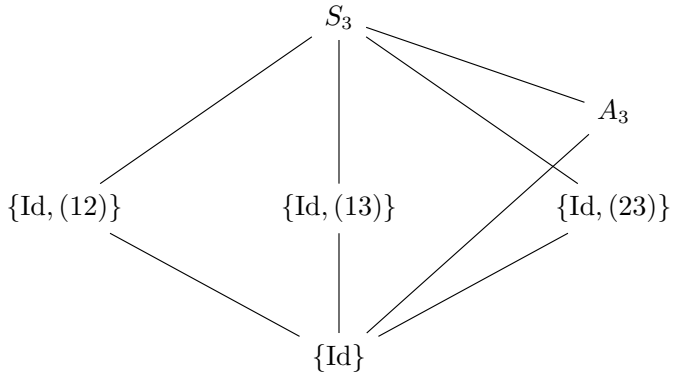
$$A_n=\{\text{偶置换}\}$$

则 $\mathrm{Ker}(\mathrm{sgn})=A_n$，由群同态基本定理，有群同构 $S_n/A_n\simeq\{-1,+1\}$，进而 $|A_n|=\frac{n!}{2}$

Fact $\mathrm{sgn}(i_1,i_2,\cdots,i_m)=(-1)^{m-1}$

证明 $(i_1i_2\cdots i_m)=(i_1i_m)\cdots(i_1i_3)(i_1i_2)$ □

例 4.40 $A_3=\{\mathrm{Id},(123),(132)\}\lhd S_3$，$S_3$ 的子群格如下



例 4.41（S_4 的正规子群） S_4 的元素如下 $(24=1+6+3+8+6)$

型	1^4	$1^2 2^1$	2^2	$1^1 3^1$	4^1
元素	Id	$(12),(13)$ $(14),(23)$ $(24),(34)$	$(12)(34)$ $(13)(24)$ $(14)(23)$	$(123),(132)$ $(124),(142)$ $(134),(143)$ $(234),(243)$	$(1234),(1243)$ $(1324),(1342)$ $(1423),(1432)$

其中型为 $1^2 2^1, 2^2$ 的元素均为二阶元，即有 9 个二阶子群

设 $N \trianglelefteq S_4$，由 Lagrange 定理知 $|N| = 12, 8, 6, 4, 3, 2, 1$，且 N 是共轭类之并，即型相同的元素一定会出现在这个子群之中，由上表可知，符合的阶数为 $12, 4$，即 S_4 有两个（真）正规子群

$$\begin{cases} K_4 = \{\mathrm{Id}, (14)(23), (13)(24), (12)(34)\} \lhd S_4 \\ A_4 = \{\text{偶置换}\} \end{cases}$$

Ex 证明 $K_4 \simeq V_4$

定义 4.4.6（单群 ,simple group）设 G 是单群，若 G 无非平凡的正规子群，即 G 的正规子群只有 $\{1_G\}, G$

Ex 设 $|G| < +\infty$ 且 G 是 Abel 群，求证：G 是单群 $\iff$ G 是 p 阶循环群

评价 $|A_5| = 60$，A_5 是单群（并非 Abel）

定理 4.4.2 $\forall n \geq 5, A_n$ 是单群

证明 分三步进行证明

Step 1. A_n 由 3-轮换生成：因为 A_n 中的元素都为偶置换，我们只需证明任意两个对换可以写为三轮换的形式：若两个对换中包含三个不同的数 i, j, k，则 $(ij)(ik) = (ikj)$；若两个对换中包含四个不同的数 i, j, k, l，则 $(ij)(kl) = (kil)(ijk)$

Step 2. 3-轮换在 A_n 中共轭：对任意 3-轮换 $(ijk), \exists \sigma \in S_n, \text{s.t. } \sigma(i) = 1, \sigma(j) = 2, \sigma(k) = 3$，若 $\sigma \in A_n$，则 $\sigma(ijk)\sigma^{-1} = (\sigma(i)\sigma(j)\sigma(k)) = (123)$；若 $\sigma \notin A_n$，即 σ 是奇置换，考虑 $(45)\sigma \in A_n$，我们有

$$(45)\sigma(ijk)\sigma^{-1}(45)^{-1} = (45)(123)(45) = (123)$$

Step 3. 设 $\{\mathrm{Id}\} \neq N \lhd A_n$，则 N 必有 3-轮换（没证，见课本），因此 N 包含所有的三轮换，由第一步知 $N = A_n$，即 A_n 没有非平凡的正规子群！ □

评价 A_4 不是单群，因为 $K_4 \lhd A_4$；$n \geq 5, S_n$ 非可解

推论 4.4.3 $n \geq 5$，则 A_n 是 S_n 的唯一非平凡正规子群

证明 设 $\{\mathrm{Id}\} \neq N \trianglelefteq S_n$，则 $(N \cap A_n) \lhd A_n$，由 A_n 是单群知 $N \cap A_n = A_n$ 或 $\{\mathrm{Id}\}$

Case 1. 若 $N \cap A_n = A_n$，则 $A_n \subset N \subset S_n$，且 $N \leq S_n$，由于 A_n 是 S_n 的最大阶真子群，且 N 是包含 A_n 的真子群，所以 $A_n = N$

Case 2. 若 $N \cap A_n = \{\mathrm{Id}\}$，则有群嵌入

$$\phi : A_n \overset{\text{inc}}{\hookrightarrow} S_n \twoheadrightarrow S_n/N$$

且 $\mathrm{Ker}\phi = N \cap A_n = \{\mathrm{Id}\}$，因此是单同态，即 $N = 2$，设 $\sigma \in N \backslash \{\mathrm{Id}\}$，则 $\mathrm{Ord}(\sigma) = 2$，因此 σ 为不交的对换之积（假设 σ 写成不交的轮换之积后，包含 3-轮换及以上，则 $\sigma^2 \neq \mathrm{Id}$），但由正规子群一定包含一整个共轭类，而 σ 所在的共轭类肯定不止一个元素，这就导出矛盾！ □

定理 4.4.3 设 $|G| < +\infty$，$C \subseteq G$ 是共轭类，则 $|C| \mid |G|$

例 4.42 是否存在 $\sigma \in A_4, \text{s.t. } \sigma(12)(34)\sigma^{-1} = (13)(24)$？

解 因为 $\sigma(12)(34)\sigma^{-1} = (\sigma(12)\sigma^{-1})(\sigma(34)\sigma^{-1}) = (\sigma(1)\sigma(2))(\sigma(3)\sigma(4))$，注意 $(abc) = (bca) = (cab)$，故可能为循环相等，具体验证即可

例 4.43 $(123), (132)$ 是否在 A_4 中共轭？

解 $\sigma(123)\sigma^{-1} = (\sigma(1)\sigma(2)\sigma(3))$，验证三种循环相等的情况！

Ex 算出 A_4 中 (123) 和 (132) 的共轭类

Ex 证明 A_4 没有 6 阶子群

§4.5 群作用

定义 4.5.1（左作用）设群 G 左作用于集合 X，记为 $G \curvearrowright X$，是指映射

$$\begin{aligned} G \times X &\xrightarrow{\psi} X \\ (g, x) &\longmapsto \psi(g, x) \overset{\text{记作}}{=\!=} g.x \in X \end{aligned}$$

满足

(1) $1_G.x = x, \forall x \in X$，即 $\psi(1_G, x) = x$

(2) $h.(g.x) = (hg).x$，即 $\psi(h, \psi(g, x)) = \psi(hg, x)$

此时称 $X \overset{\text{def}}{=} (X, \psi)$ 为左 G-集

Fact 任给群同态 $G \xrightarrow{\rho} S(Y)$，则有左作用 $G \curvearrowright Y$

$$g.y = \rho(g)(y)$$

Ex 验证上述确实为左作用

Fact 给定左 G-集 (X, ψ)，则有

$$\begin{aligned} \rho : G &\longrightarrow S(X) \\ g &\longmapsto \rho(g) \end{aligned}$$

其中

$$\begin{aligned} \rho(g) : X &\longrightarrow X \\ x &\longmapsto g.x \end{aligned}$$

接下来验证 ρ 是群同态，即 ρ 保乘法：$\rho(gh) = \rho(g)\rho(h)$

$$\begin{cases} \rho(gh) = (gh).x \\ \rho(g) \circ \rho(h) = \rho(g)(h.x) = g.(h.x) = (gh).x \end{cases}$$

我们将上述事实总结为如下定理

定理 4.5.1 设有群作用 $G \curvearrowright X$，则存在双射

$$\begin{aligned} \{G在X上的左作用\} &\xleftrightarrow{1:1} \mathrm{Hom}(G, S(X)) \\ G \curvearrowright X &\longmapsto [\rho : G \to S(X), x \mapsto g.x] \\ [G \curvearrowright X : g.y = \rho(g)(y)] &\longmapsto \rho \end{aligned}$$

其中 $\mathrm{Hom}(G, S(X))$ 表示 G 到 $S(X)$ 的群同态全体

评价 给定左作用，我们通常研究它对应的 $\rho : G \to S(X)$. 思考右作用 $X \curvearrowleft G$ 如何定义？

定义 4.5.2（群作用的核）定义群作用的核 N 为它所对应的群同态 $\rho : G \to S(X)$ 的核，即 $N = \mathrm{Ker}\rho$，所以

$$\begin{aligned} a \in G是这个作用的核 &\iff a \in \mathrm{Ker}\rho \iff \rho(a) = \mathrm{Id}_{S(X)} \\ &\iff \forall x \in X, \rho(a)(x) = x \iff \forall x \in X, a.x = x \end{aligned}$$

例 4.44 $S(X) \curvearrowright X$

$$\begin{aligned} S(X) \times X &\xrightarrow{\psi} X \\ (\sigma, x) &\longmapsto \sigma(x) \end{aligned}$$

称 (X, ψ) 为左 $S(X)$-集

例 4.45 考虑域扩张 K/k，$\mathrm{Aut}(K/k)\curvearrowright K$

$$\begin{aligned}\mathrm{Aut}(K/k)\times K &\xrightarrow{\psi} K\\ (\sigma,a)&\longmapsto \sigma(a)\end{aligned}$$

例 4.46 $\mathrm{GL}(V)\curvearrowright V$，其中 V 是线性空间

$$\begin{aligned}\mathrm{GL}(V) &\xrightarrow{\psi} V\\ (A,x)&\longmapsto Ax\end{aligned}$$

称为左线性作用

定义 4.5.3（轨道 ,orbit）给定 $G\curvearrowright X$，定义

1. x 的 G-轨道，G-orbit
$$\mathcal{O}_x=\{g.x|g\in G\}\subseteq X$$
2. X 上有等价关系
$$x\approx y \iff \exists g\in G,\text{s.t. } y=g.x$$
即 $\mathcal{O}_x$ 为 x 所在的等价类（若 $y=g.x$，则 $g^{-1}.y=g^{-1}.(g.x)=(g^{-1}g).x=1.x=x$）
3. 有 X 的 G-轨道分解
$$X=\bigsqcup_{x\in I}\mathcal{O}_x$$
其中 I 为轨道的完全代表元系（每个轨道中取一个代表元）

定义 4.5.4（可迁 ,transitive)称 $G\curvearrowright X$ 可迁,若仅有一个 G-轨道,即对 $\forall x,y\in X,\exists g\in G,\text{s.t. } y=g.x$

Fact 给定左作用 $G\curvearrowright X$, 它的限制作用 $G\curvearrowright\mathcal{O}_x$ 是可迁的

证明 这是因为 $\mathcal{O}_x$ 的定义, 即对 $\forall y\in\mathcal{O}_x,\exists g\in G,\text{s.t. } y=g.x$ □

定义 4.5.5（稳定化子 ,stablizer）设 $G\curvearrowright X$，定义 $x\in X$ 的稳定化子为

$$G_x=\{g\in G|g.x=x\}$$

可以验证 $G_x\leq G$ 为子群

引理 4.5.1 设 $G\curvearrowright X,x,y\in X$，若 $\exists h\in G,\text{s.t. } x=h.y$，则

$$G_x=hG_yh^{-1}$$

即同一轨道中不同元素的稳定化子是相互共轭的

证明 对 $\forall g\in G_x, g.x=x$, 又因为 $x=h.y$, 所以 $y=h^{-1}.x$

$$(h^{-1}gh).y=(h^{-1}g).(h.y)=(h^{-1}g).x=h^{-1}.(g.x)=h^{-1}.x=y$$

所以 $h^{-1}gh\in G_y$, 即 $g\in hG_yh^{-1}$; 反之假设 $g\in hG_yh^{-1}$, 则 $h^{-1}gh\in G_y$, 即 $(h^{-1}gh).y=y$, 所以

$$y=(h^{-1}gh).y=(h^{-1}g).(h.y)=(h^{-1}g).x\Longrightarrow x=h.y=h.(h^{-1}g.x)=g.x$$

因此 $g\in G_x$, 所以二者相等 □

评价 因此 $G_x\simeq G_y$，它们的阶相同

例 4.47（左诱导作用）给定 $H\leq G$，考虑 $G/H=\{aH|a\in G\}$（不一定是商群，此时只表示左陪集的全体），则 $G\curvearrowright G/H$

$$g.(aH)=gaH$$

记为左诱导作用，它是可迁的；特别地取 $H=\{1_G\}$，此时称为左正则作用

Ex $G_{aH}=aHa^{-1},\forall a\in G$

例 4.48 $S_n\curvearrowright\{1,2,\cdots,n\}$ 可迁，对 $\forall 1\leq i\leq n$，它的稳定化子 $\simeq S_{n-1}$

例 4.49 $\forall\sigma\in S_n$，它的生成子群 $(\sigma)\leq S_n$，有群作用 $G=(\sigma)\curvearrowright\{1,2,\cdots,n\}$，它的 G-轨道？

例 4.50 给定域扩张 K/k，考虑 $\mathrm{Aut}(K/k)\curvearrowright K$

$$\sigma.a=\sigma(a),\quad \forall a\in K,\sigma\in\mathrm{Aut}(K/k)$$

$\forall f(x)\in k[x],\mathrm{Root}_K(f)=\{a\in K|f(a)=0\}$ 是一个有限集，我们可以将群作用限制在 $\mathrm{Root}_K(f)$ 中，因为 $\sigma(a)\in\mathrm{Root}_K(f)$

更进一步，取 K/k 为 $f(x)$ 的分裂域，则 $\mathrm{Aut}(K/k)\curvearrowright\mathrm{Root}_K(f)$ 有群同态

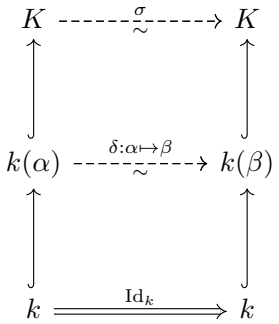
$$\begin{aligned}\mathrm{Aut}(K/k)&\xrightarrow{\rho}S(\mathrm{Root}_K(f))\\ \sigma&\longmapsto\sigma|_{\mathrm{Root}_K(f)}\end{aligned}$$

(1) ρ 是单射

Proof : 验证 $\mathrm{Ker}(\rho)=\{\mathrm{Id}\}$，即验证若 $\sigma|_{\mathrm{Root}_K(f)}=\mathrm{Id}$，则 $\sigma=\mathrm{Id}_K$

(2) 若 $f(x)$ 在 k 上不可约，则 ψ 是可迁的，即 $\forall a,b\in\mathrm{Root}_k(f)$，存在 $\exists\sigma\in\mathrm{Aut}(K/k),\text{s.t. }\sigma(a)=b$

Proof : 考虑延拓定理，因为 $a,b\in\mathrm{Root}_K(f)$，所以存在 Id_k 的延拓 $\delta:k(\alpha)\xrightarrow{\sim}k(\beta)$ 满足 $\delta(\alpha)=\beta$，由 K/k 是 f 的分裂域知，可将 δ 延拓到 K 上的域同构 σ，且 $\sigma|_{k(\alpha)}=\delta$，如下图



例 4.51 $\mathrm{GL}_2(\mathbb{F}_2)=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\middle|a,b,c,d\in\mathbb{F}_2\right\}$，有群作用 $G=\mathrm{GL}_2(\mathbb{F}_2)\curvearrowright(\mathbb{F}_2)^2\overset{\text{记作}}{=\!=}V$

$$\begin{pmatrix}a&b\\c&d\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}ax+by\\cx+dy\end{pmatrix}$$

有两个 G-轨道：$\left\{\begin{pmatrix}\bar0\\\bar0\end{pmatrix}\right\},\left\{\begin{pmatrix}\bar0\\\bar1\end{pmatrix},\begin{pmatrix}\bar1\\\bar0\end{pmatrix},\begin{pmatrix}\bar1\\\bar1\end{pmatrix}\right\}\overset{\text{def}}{=}X$

Ex 证明存在群同构 $\rho:G\to S(X)$

定理 4.5.2 设有左作用 $G\curvearrowright X$，对 $\forall x\in X$，存在双射

$$\begin{aligned}f:G/G_x&\overset{1:1}{\longleftrightarrow}\mathcal{O}_x\\aG_x&\longmapsto a.x\end{aligned}$$

实际上是 G-集间的同构

评价 对集合间的双射 $X\overset{f}{\to}Y$，以及群作用 $G\curvearrowright X,G\curvearrowright Y$，称 f 与 G-作用相容，若

$$f(g.x)=g.(f(x)),\quad\forall x\in X,g\in G$$

因此 $G/G_x\to\mathcal{O}_x$ 实际上是 G-集的双射，即

- $G/G_x\overset{f}{\to}\mathcal{O}_x$ 是双射
- 相容性：$\begin{cases}f(g.hG_x)=f(ghG_x)=gh.x\\g.(f(hG_x))=g.(h.x)=gh.x\end{cases}$

证明 良定性：设 $aG_x=bG_x$，则 $b^{-1}a\in G_x,\exists h\in G_x,\text{s.t. }a=bh$，故

$$a.x=(bh).x=b.(h.x)=b.x$$

所以映射是良定的，且它是单射，假设 $a.x=b.x$，则 $(b^{-1}a).x=x\Longrightarrow b^{-1}a\in G_x\Longrightarrow aG_x=bG_x$

最后由定义，它显然是满射 □

推论 4.5.1（轨道-稳定化子公式）

$$|G|=|\mathcal{O}_x|\cdot|G_x|$$

特别地，$|\mathcal{O}_x|\ \big|\ |G|$

定义 4.5.6（忠实作用）设 $G\curvearrowright X$ 是忠实的，若 $\forall1_G\neq g\in G,\exists x\in X,\text{s.t. }g.x\neq x$；换句话说，称 $G\curvearrowright X$ 是忠实的，则定理 4.5.1 中对应的群同态

$$\begin{aligned}\rho:G&\longrightarrow S(X)\\g&\longmapsto\rho(g)=g.x\end{aligned}$$

是单射, 也等价于说群作用 $G\curvearrowright X$ 的核 $N=\mathrm{Ker}\rho=\{1_G\}$

Ex 证明 $\mathrm{Ker}\rho=\bigcap\limits_{x\in X}G_x$

例 4.52 左正则作用 $G\curvearrowright G$

$$\begin{aligned}G\times G&\longrightarrow G\\(g,a)&\longmapsto g.a=ga\end{aligned}$$

是忠实的. 因此有 Cayley 定理: $G\hookrightarrow S(G)$ 是单射（进而 G 与 $S(G)$ 的一个子群同构）

定义 4.5.7（自由作用）称 $G\curvearrowright X$ 是自由的, 若 $G_x=\{1_G\},\forall x\in X$. 此时 $|\mathcal{O}_x|=|G|$, 进而

$$|X|=\sum_{i\in I}|\mathcal{O}_x|\Longrightarrow|G|\ \big|\ |X|$$

例 4.53 设 $H\leq G$, 考虑左正则作用 $H\curvearrowright G$

$$\begin{aligned}H\times G&\longrightarrow G\\(h,a)&\longmapsto h.a=ha\end{aligned}$$

它是自由作用, 因为 $\forall a\in G$

$$G_a=\{h\in H:ha=a\}=\{1_H\}$$

因此 $|H|\ \big|\ |G|$, 再次证明了拉格朗日定理

定义 4.5.8（平凡群作用）称 $G\curvearrowright X$ 是平凡的, 若 $\forall g\in G,x\in X,g.x=x$, 即 $G_x=G$. 此时 $\rho:G\to S(X),\forall g\mapsto \mathrm{Id}_X$

例 4.54 $G\curvearrowright X$, 它的不动点集为

$$X^G=\{x\in X|g.x=x,\forall g\in G\}$$

若 $X^G\neq\varnothing$, 则 $G\curvearrowright(X^G)$ 是平凡的

定义 4.5.9（共轭作用）共轭作用定义为 $G\curvearrowright X=G$

$$\begin{aligned}G\times G&\longrightarrow G\\(g,x)&\longmapsto gxg^{-1}\end{aligned}$$

(1) 共轭作用是平凡的 $\Longleftrightarrow$ G 是 *Abel* 群
(2) $x\in G$ 的（共轭）轨道为 x 的共轭类, 记为

$$C_x=\{gxg^{-1}|g\in G\}$$

由轨道-稳定化子公式知 $|C_x| \mid |G|$

(3) $C_x = \{x\} \iff x \in Z(G)$, 其中 $Z(G)$ 为群 G 的中心

(4) x 的稳定化子为 $Z(x) = \{g \in G | gx = xg\} = \{g \in G | gxg^{-1} = x\} \leq G$, 称为 x 的中心化子

Ex $Z(G) = \bigcap\limits_{x \in G} Z(x)$

推论 4.5.2（共轭作用下的轨道-稳定化子公式）在共轭作用下,$Z(x)$ 为 x 的稳定化子/中心化子,C_x 为 x 的轨道/共轭类, 则

$$|G| = |C_x| \cdot |Z(x)|$$

命题 4.5.1（类公式）按共轭类的元素个数多少分为两种: 个数 ≤ 1 和 > 1

$$|G| = |Z(G)| + \sum_{x:|C_x|>1} |C_x|$$

例 4.55 计算 $A_4 \ni (123)$ 的共轭类的大小 $|C_{(123)}|$

因为 $|A_4| = |C_{(123)}| \cdot |Z\big((123)\big)|$, 显然任意一个元素, 它都在自己的中心化子中, 即 $(123) \in Z\big((123)\big)$, 所以 $\big((123)\big) \subset Z\big((123)\big) \Longrightarrow Z\big((123)\big) \geq 3$, 又因为

$$\sigma(123)\sigma^{-1} = (\sigma(1)\sigma(2)\sigma(3)) = (123)$$

该方程至多只有三组解, 所以 $Z\big((123)\big) = 3$, 进而 $|C_{(123)}| = \frac{12}{3} = 4$

定义 4.5.10（p 群）设 p 是素数, 称 G 为 p-群, 若 $|G| = p^n, n \geq 1$

评价 若 $|G| = p$, 则 $G \simeq \mu_p$, 即 G 是循环群

命题 4.5.2 p-群一定有非平凡中心

证明 设 $|G| = p^n$, 则 $|Z(G)| = p^r, r > 0$, 若 $|Z(G)| = 1$, 由类等式得

$$|G| = 1 + \sum_{|C_x|>1} |C_x|$$

又因为 $|C_x| \mid p^r, |C_x| > 1$, 故 $p \mid C_x$, 这就导致上式左边是 p 的倍数, 右边不是 p 的倍数, 矛盾 □

命题 4.5.3 p^2 阶群是 Abel 群, 且同构于 $(\mathbb{Z}_{p^2}, +)$ 或 $\mathbb{Z}_p \times \mathbb{Z}_p$

证明 因为 p 群一定有非平凡中心, 所以 $\exists 1 \neq g \in Z(G)$, 则 $\mathrm{Ord}(g) = p$ 或 p^2

Case 1. $\mathrm{Ord}(g) = p^2$, 则 $G \simeq (\mathbb{Z}_{p^2}, +)$

Case 2. $\mathrm{Ord}(g)=p$, 则 $H=(g)=\{1,g,\cdots,g^{p-1}\}\leq G$, 取 $g_1\notin H$, s.t. $\mathrm{Ord}(g_1)=p$（否则 $\mathrm{Ord}(g_1)=p^2$, 回到 Case 1.）, 则 $(g,g_1)=G$（由 Lagrange 定理, 因为 $p+1\leq|(g,g_1)|\leq p^2$, 且 $|(g,g_1)|\mid|G|=p^2$, 所以 $(g,g_1)=G$）. 实际上由 $g\in Z(G)$ 知

$$(g,g_1)=\{g^ig_1^j|0\leq i,j\leq p-1\}$$

记 $K=(g_1)$, 考虑映射

$$\begin{aligned}\Phi:H\times K&\longrightarrow G\\(h,k)&\longmapsto hk\end{aligned}$$

由下面的练习即得证 □

Ex 证明 Φ 是同态

例 4.56 考虑共轭作用

$$S_4\curvearrowright X=\{(12)(34),(13)(24),(14)(23)\},\quad g.x=gxg^{-1}$$

则有群同态 $S_4\xrightarrow{\rho}S(X)\simeq S_3$

Ex 算 $\mathrm{Ker}\rho$

例 4.57 设 $H\leq G$, 考虑群作用

$$G\curvearrowright X_H=\{H'\leq G|H'与H共轭\},\quad g.H'=gH'g^{-1}$$

H 的稳定化子为

$$H\subseteq N_G(H)=\{g\in G|gHg^{-1}=H\}$$

也称为 H 的正规化子

Fact

$$\begin{aligned}H\trianglelefteq G&\iff N_G(H)=G\\&\iff X_H=\{H\}\end{aligned}$$

且我们有 $|G|=|X_H|\cdot|N_G(H)|$

§4.6 Sylow 定理

定义 4.6.1（Sylow 子群）设 $|G|=p^rm,p\nmid m$, 子群 $P\leq G$ 称为 G 的 Sylow p-子群, 若 $|P|=p^r$

评价 $[G:P]=m$

定理 4.6.1（Sylow 定理）设 $|G|=p^rm,m\nmid m,r\geq1$, 则

(1) Sylow p-子群总存在

(2) Sylow p 子群间相互共轭

(3) Sylow p-子群的个数为 m 的因子, 且形如 $kp+1$

(4) $\forall p$-子群 $B \leq G$, 总存在某个 Sylow p-子群 P, s.t. $B \subset P$

证明 只证明 Sylow p-子群的存在性. 设 $|G| = p^r m, p \nmid m$

Claim: $\exists P \leq G, |P| = p^r$

考虑所有 G 的 p^r 阶子集全体 $X = \{U \subset G : |U| = p^r\} \subset \mathcal{P}(G)$, 考虑左正则作用 $G \curvearrowright X$

$$\begin{aligned} G \times X &\longrightarrow X \\ (g, U) &\longmapsto g.U = gU \end{aligned}$$

注意到

$$|X| = \binom{p^r m}{p^r} = \frac{p^r m(p^r m - 1)\cdots(p^r m - p^r + 1)}{p^r(p^r - 1)\cdots 1}$$

对 $\forall 1 \leq j \leq p^k - 1$, 设 $j = p^t j_1$, 其中 $(p, j_1) = 1$, 则

$$\begin{cases} p^r m - j = p^r m - p^t j_1 = p^t(p^{r-t} m - j_1) \\ p^r - j = p^r - p^t j_1 = p^t(p^{r-t} - j_1) \end{cases}$$

因为 $(p, j_1) = 1$, 所以 $p \nmid p^{r-t} m - j_1, p \nmid p^{r-t} - j_1$, 故 $p \nmid \frac{p^{r-t} m - j_1}{p^{r-t} - j_1} = \frac{p^r m - j}{p^r - j}$, 所以 $p \nmid |X|$.

将 X 写为轨道的无交并

$$X = \bigsqcup_{U \in I} \mathcal{O}_U$$

则 $\exists U$, s.t. $p \nmid |\mathcal{O}_U|$, 考虑 $G_U = \{g \in G | gU = U\} \leq G$, 由轨道-稳定化子公式

$$|G| = |G_U| \cdot |\mathcal{O}_U|$$

因此 $G_U = p^r \cdot m', m' \mid m$

此外, 考虑群作用 $G_U \curvearrowright U$

$$\begin{aligned} G_U \times U &\longrightarrow U \\ (g, x) &\longmapsto g.x = gx \end{aligned}$$

它是自由作用, 因为由 $gU = U$ 知,$\forall g \in G_U, x \in U, \exists! y \in U$, s.t. $gx = y$, 即 $\forall x \in U, G_x = \{g \in G_U | gx = x\} = \{1_G\}$. 因此 $|G_U| \mid |U| = p^r$, 所以 $|G_U| = p^r$, 故 G_U 就是我们要找的 Sylow p-子群 □

证明 (Sylow p-子群的存在性, 另证)

Step 1. 由 Cayley 定理, 存在群嵌入 $G \hookrightarrow S(G) \simeq S_n$ 且还有 $S_n \hookrightarrow \mathrm{GL}_n(\mathbb{F}_p)$, 故有群嵌入 $G \hookrightarrow \mathrm{GL}_n(\mathbb{F}_p)$

Step 2. 计算 $|\mathrm{GL}_n(\mathbb{F}_p)| = p^{\frac{n(n-1)}{2}} \cdot m, p \nmid m$

Step 3. 由线性代数的知识, 考虑对角元均为 1 的上三角阵构成的集合

$$U = \left\{ \begin{pmatrix} 1 & * & * \\ & \ddots & * \\ & & 1 \end{pmatrix} \right\}$$

显然它的阶为 $p^{\frac{n(n-1)}{2}}$, 故它是 $\mathrm{GL}_n(\mathbb{F}_p)$ 的 Sylow p-子群

Step 4. 将 G 视为 $\mathrm{GL}_n(\mathbb{F}_p)$ 的子群, 由下面的练习即证 □

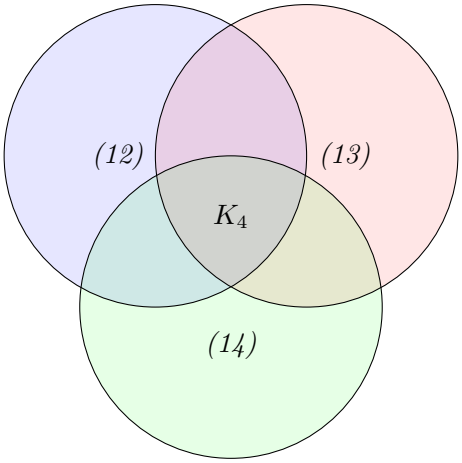
Ex 验证 $|\mathrm{GL}_n(\mathbb{F}_p)| = \prod_{k=1}^{n}(p^n - p^{k-1})$

Ex 设 $H \le K, U \le K$ 是 K 的 Sylow p-子群, 则 $\exists g \in K, \text{s.t. } H \cap gUg^{-1}$ 为 H 的 Sylow p-子群

Hint: 考虑群作用 $H \curvearrowright (K/U)$

例 4.58 $|S_4| = 24 = 3^1 2^3$, 恰有 4 个 Sylow 3-子群

考虑 S_4 的 Sylow 2-子群, 即 8 阶子群, 由 Sylow 定理知 $|8\text{阶子群}| = \begin{cases} 3 \text{ 的因子} \\ 2k+1 \end{cases}$, 故恰有 3 个 Sylow 2-子群, 且它们三个相交即为 K_4



命题 4.6.1 108 阶群非单群

证明 因为 $|G| = 108 = 2^2 3^3$, 则 Sylow 3-子群, 即 27 阶子群总存在, 取 $P \le G, \text{s.t. } |P| = 27$, 考虑左诱导作用

$$G \curvearrowright G/P, \quad (g, aP) = gaP$$

则有群同态

$$\rho : G \longrightarrow S(G/P) \simeq S_4$$
$$g \longmapsto \rho(g) : aP \mapsto gaP$$

由群同态基本定理 $G/\mathrm{Ker}\rho \simeq \mathrm{Im}\rho$ 因为

(1) $\mathrm{Im}\rho \neq \{\mathrm{Id}_{S(G/P)}\}$, 否则 $\forall g \in G, \rho(g) = \mathrm{Id}_{S(G/P)}$, 那么对 $\forall a, g \in G$ 就有 $gaP = aP \Longrightarrow a^{-1}ga \in P$, 显然矛盾! 所以 $\mathrm{Ker}\rho \neq G$

(2) $\mathrm{Im}\rho \le S(G/P)$, 故 $|\mathrm{Im}\rho| \le |S(G/P)| = 24$, 所以 $\mathrm{Ker}\rho \neq \{1_G\}$

所以 $\mathrm{Ker}\rho \trianglelefteq G$, 故 108 阶群非单群 □

命题 4.6.2 $|G| = 35$, 则 G 循环

证明 因为 $|G|=35=5\times 7$, 则

$$\begin{cases} |5\text{阶子群}| = \begin{cases} 7\text{的因子} \\ 5k+1 \end{cases} & =1 \\ |7\text{阶子群}| = \begin{cases} 5\text{的因子} \\ 7k+1 \end{cases} & =1 \end{cases}$$

则 $\exists! P,Q\lhd G,|P|=5,|Q|=7$, 且由于 5,7 阶子群个数为 1 知,$P,Q$ 一定正规. 考虑

$$\begin{aligned} \phi: P\times Q &\longrightarrow G \\ (h,g) &\longmapsto hg \end{aligned}$$

可以证明 $P\cap Q=\{1_G\}$, 由下面的练习即得证 □

Ex 证明上述 ϕ 是同态

例 4.59 设 $|G|=p_1^{s_1}\cdots p_t^{s_t}$, 其中 p_i 为两两不同的素数, 若 G 是 Abel 群, 则存在唯一 Sylow p_i-子群 P_i, 使得如下群同构成立

$$\begin{aligned} P_1\times P_2\times\cdots\times P_t &\xrightarrow{\sim} G \\ (a_1,a_2,\cdots,a_t) &\longmapsto a_1a_2\cdots a_t \end{aligned}$$

Ex 证明上面的群同构

评价 有限 Abel 群的结构问题归结于 Abel p-群的结构问题

定理 4.6.2（Cauchy）设 $p\mid |G|$, 则 G 有 p 阶元, 进而 G 有 p 阶子群

证明 由 Sylow 定理,G 有 Sylow p-子群 P, 设 $|P|=p^r$, 任取 $g\in P\backslash\{1_G\}$, 则 $\mathrm{Ord}(g)=p^a,1\le a\le r$

Claim: $\mathrm{Ord}(g^{p^{a-1}})=p$

一方面 $(g^{p^{a-1}})^p=g^{p^a}=1$, 故 $\mathrm{Ord}(g^{p^{a-1}})\mid p$. 另一方面设 $\mathrm{Ord}(g)=d$, 则

$$(g^{p^{a-1}})^d=g^{dp^{a-1}}=1\Longrightarrow p^a\mid dp^{a-1}\Longrightarrow p\mid d$$

因此 $\mathrm{Ord}(g^{p^{a-1}})=p$ □

例 4.60 设 $|G|=56$, 则 G 非单

证明 因为 $|7\text{阶子群}|=\begin{cases} 8\text{ 的因子} \\ 7k+1 \end{cases}=1\text{或}8$

Case 1. 仅有一个 7 阶子群, 则它一定是正规子群

Case 2. 有 8 个 7 阶子群 $H_1,\cdots,H_8$, 因为 7 阶群一定是循环群, 所以 $H_i\cap H_j=\{1_G\}$, 否则 $H_i=H_j$. 因此

$$|H_1\cup\cdots\cup H_8|=1+(7-1)\times 8=49$$

这上面 49 个元素, 除了 1, 其余元素阶数均为 7. 又由 Sylow 定理,G 一定有 Sylow 2-子群, 即 8 阶子群, 而 8 阶群中元素的阶不可能为 7, 所以除去上面 49 个元素, 剩下的 7 个元素加上 1_G 恰好构成 G 的 Sylow 2-子群 $Q\lhd G$, 且由上分析知 Q 恰只有一个, 故 Q 是正规子群 □

§4.7 自由群与群的表示

目标: 将任意群 G 表示为 $G = F/N, F$ 是自由群,$N \lhd F$

定义 4.7.1（字）设 $X \neq \varnothing$, 考虑 X 的形式逆 $X^{-1} = \{x^{-1} | x \in X\}$, 称 $X \sqcup X^{-1}$ 为字母集合, 定义

1. 字 Word
$$w = x_1 x_2 \cdots x_n, \quad x_i \in X \sqcup X^{-1}$$
2. 字 ω 称为即约的 reduced, 若 $x_i \neq x_{i-1}^{-1}, \forall i \geq 2$, 即相邻元素不能消去
3. 称即约的两个字 $x_1 \cdots x_n, y_1 \cdots y_m$ 相等, 若 $n = m, x_i = y_i, \forall i$
4. 若 $n = 0$, 定义 $\omega = 1$ 为空字

评价 约定 $x^2 = xx$, 其余幂次类似

例 4.61 设 $X = \{x, y\}, xyx^{-1}y$ 是即约的, $xyy^{-1}x$ 不即约, 它的即约形式为 x^2

Fact 任意字可以约化为唯一的即约字

Ex 证明上述事实, voluntary

例 4.62 $xy^{-1}yy^{-1}xxx^{-1}y = xy^{-1}xy$

定义 4.7.2（自由群）集合 X 的自由群

$$\begin{aligned} F(X) &= \{\text{所有以} X \sqcup X^{-1} \text{中元素构成的字}\} \\ &= \{x_1 \cdots x_n | x_i \in X \sqcup X^{-1}, 1 \leq i \leq n, n \in \mathbb{N}\} \end{aligned}$$

自由群的结合律蕴含了即约的唯一性. 它的乘法规定为字的连接以及即约化

若 $|X| < +\infty$, 我们称 $F(X)$ 为有限生成自由群

评价 $(w_1 \cdot w_2) \cdot w_3$ 和 $w_1 \cdot (w_2 \cdot w_3)$ 是否相等? 本质上化为 $w_1 w_2 w_3$ 经过约化后表达是否唯一, 这点由上面的事实保证

例 4.63 $(xyx) \cdot (x^{-1}y^{-1}x) = x^2$

例 4.64 若 $X = \{a\}$, 则
$$F(X) = \{\cdots, a^{-2}, a^{-1}, 1, a, a^2, \cdots\} \simeq (\mathbb{Z}, +)$$

一个元素的集合的自由群同构于无限循环群

例 4.65 若 $X = \{x, y\}$, 则

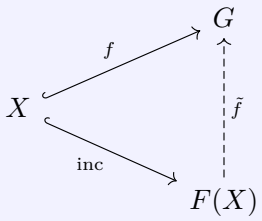
$$F(X) = \left\{ \begin{array}{c} 1 \\ x, y, x^{-1}, y^{-1} \\ x^2, y^2, x^{-2}, y^{-2}, xy, yx, x^{-1}y, yx^{-1}, xy^{-1}, yx^{-1}, x^{-1}y^{-1}, y^{-1}x^{-1} \\ \cdots\cdots\cdots \end{array} \right\}$$

长度为 2 的字有 12 个; 长度为 3 的字有 36 个

命题 4.7.1（自由群的泛性质）给定群 G 以及集合 X, 对任意映射 $f : X \to G$, 可将 f 唯一延拓为群同态

$$\tilde{f} : F(X) \longrightarrow G$$

使得 $\tilde{f}|_X = f$, 即下面的图交换



证明 存在性：对 $\forall x \in X$, 定义 $\tilde{f}(x) = x, \tilde{f}(x^{-1}) = f(x)^{-1}$, 给定一个字 $x_1 \cdots x_n$, 定义

$$\tilde{f}(x_1 \cdots x_n) = \tilde{f}(x_1) \cdots \tilde{f}(x_n)$$

□

推论 4.7.1 任意群 G 都是某个自由群的商群

证明 取 $X \subset G$ 是 G 的生成元集, 考虑群嵌入 $\mathrm{inc} : X \hookrightarrow G$, 由泛性质知, 存在 inc 的延拓

$$\widetilde{\mathrm{inc}} : F(X) \to G$$

由 X 是 G 的生成元集知它是满射, 由群同态基本定理知,G 与 $F(X)$ 的某个商群同构 □

定义 4.7.3（群的有限表现）群的有限表现是指

$$G = < x_1, \cdots, x_n \mid r_1, \cdots, r_m >$$

其中 $x_1, \cdots, x_n$ 为生成元,$r_i \in F(x_1, \cdots, x_n)$ 是关系, 即为由生成元组成的字, 定义为

$$F(x_1, \cdots, x_n)/N(r_1, \cdots, r_m)$$

其中 $N(r_1, \cdots, r_m)$ 是包含 $r_1, \cdots, r_m$ 的 $F(x_1, \cdots, x_n)$ 的最小正规子群, 实际上根据商群的定义,G 也可以写为

$$G = < x_1, \cdots, x_n \mid r_1 = 1, \cdots, r_m = 1 >$$

Ex 证明 $N(r_1, \cdots, r_m) = (\omega r_j \omega^{-1} \mid 1 \le j \le m, \omega \in F(x_1, \cdots, x_n))$

命题 4.7.2 设 $G=<x_1,\cdots,x_n \mid r_1,\cdots,r_m>$, 记 $X=\{x_1,\cdots,x_n\}$, 设 H 是群, 若有映射

$$f: X \to H$$

则 f 可延拓为群同态 $G \xrightarrow{\tilde{f}} H \iff f(x_1),\cdots,f(x_n)$ 在 H 中满足关系 $r_1,\cdots,r_m$

例 4.66 $<g \mid g^d>=F(g)/N(g^d)\simeq \mu_d$, 设 H 是群, 考虑映射

$$\begin{aligned} f:\{g\} &\longrightarrow H \\ g &\longmapsto f(g) \end{aligned}$$

由命题 4.7.2,f 可延拓为 $\tilde{f}: F(g)\to H$ 当且仅当 $\tilde{f}(g)=f(g)$ 在 H 中满足关系 g^d, 即 $f(g)^d=1_H$ 且我们有 $N(g^d)\subset \mathrm{Ker}(\tilde{f})$

例 4.67 $G=<x,y \mid x^2,y^2,(xy)^3>=F(x,y)/N(x^2,y^2,(xy)^3)$

Claim: 任意群 H, 任意映射 $f:\{x,y\}\to H, x\mapsto f(x), y\mapsto f(y)$, 若 $f(x)^2=1_H, f(y)^2=1_H, \big(f(x)f(y)\big)^3=1_H$, 则存在唯一群同态

$$\begin{aligned} \tilde{f}: G &\longrightarrow H \\ \bar{x} &\longmapsto f(x) \\ \bar{y} &\longmapsto f(y) \end{aligned}$$

此时视 $G=F(x,y)/N(x^2,y^2,(xy)^3)$ 为商群, 其中 $\bar{x}=xN, \bar{y}=yN$

评价 由商群的定义,$\bar{x}^2=\bar{1}, \bar{y}^2=\bar{1}, (\bar{x}\bar{y})^3=1$, 可以验证 $G\simeq S_3$, 此外 G 还可以写为

$$\begin{aligned} G &=<a,b \mid a^2=1=b^2, aba=bab> \\ &=<a,b \mid a^2,b^2,abab^{-1}a^{-1}b^{-1}> \end{aligned}$$

评价 天才不坐在教室里

Fact 设 $G=<x,y \mid x^2,y^2,(xy)^3>$, 证明 $G\simeq S_3$

证明 考虑

$$\begin{aligned} \{x,y\} &\xrightarrow{f} S_3 \\ x &\longmapsto (12) \\ y &\longmapsto (13) \end{aligned}$$

由泛性质, 存在 f 的延拓

$$\begin{aligned} F(x,y) &\xrightarrow{\tilde{f}} S_3 \\ x &\longmapsto (12) \\ y &\longmapsto (13) \end{aligned}$$

因为 $x^2\mapsto (12)^2=\mathrm{Id}, y^2\mapsto (13)^2=\mathrm{Id}, (xy)^3\mapsto \mathrm{Id}$, 所以 $N(x^2,y^2,(xy)^3)\subset \mathrm{Ker}\tilde{f}$, 则 $\tilde{f}$ 诱导满射, 此处

仍记为 $\tilde{f}$

$$\begin{aligned}\tilde{f}: F(x,y)/N(x^2,y^2,(xy)^3) &\longrightarrow S_3\\ \overline{x} &\longmapsto (12)\\ \overline{y} &\longmapsto (13)\end{aligned}$$

记 $G = F(x,y)/N(x^2,y^2,(xy)^3)$

Claim: $G = \{\overline{1}, \overline{x}, \overline{y}, \overline{xy}, \overline{yx}, \overline{xyx}\}$

对 $\forall \omega \in LHS$, 若 ω 的长度小于等于 2, 则 $\omega = \overline{1}, \overline{x}, \overline{y}, \overline{xy}, \overline{yx}$ 首先有 $\overline{x}^{-1} = \overline{x}, \overline{y}^{-1} = \overline{y}$, 若 ω 的长度小于等于 2, 则 $\omega = \overline{1}, \overline{x}, \overline{y}, \overline{xy}, \overline{yx}$ 因此长度大于 2 的元素一定形如

$$\overline{\omega} = \overline{xyxyxyxyx}\cdots \text{ 或 } \overline{yxyxyxyxy}\cdots$$

再利用 $(\overline{xy})^3 = 1$ 知, 长度大于 2 的元素只能是 $\overline{xyx} = \overline{yxy}$（因为长度为 4,5 的元素可以进一步化简）, 故群 G 的大小 $|G| \leq 6$, 所以断言得证 □

例 4.68 $D_6 = \{g \in \mathrm{O}_2 \mid g$保正六边形$\}$, 其中共有 6 个旋转,6 个对称

1. 设 $a \in D_6, \mathrm{Ord}(a) = 6$ 为旋转的生成元, 则六个旋转为 $a, a^2, \cdots, a^5, a^6 = \mathrm{Id}$
2. 设 $b = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, b^2 = 1$, 则 $b, ba, \cdots, ba^{6-1}$ 均为对称（行列式为 -1）

因此我们找到了 D_6 的生成元 a, b, 它们满足 $a^6 = 1, b^2 = 1, (ba)^2 = 1$

定义 $G =< x, y \mid x^6, y^2, (xy)^2 >= F(x,y)/N(x^6, y^2, (xy)^2)$, 它的生成元为 $\overline{x}, \overline{y}$

接下来证明 $G \simeq D_6$

Step 1. 考虑满射

$$\begin{aligned} f: G &\longrightarrow D_6\\ \overline{x} &\longmapsto a\\ \overline{y} &\longmapsto b\end{aligned}$$

Step 2. 证明 $|G| \leq 12$

Claim: $G = \{\overline{x}^i\overline{y}^j \mid 0 \leq i \leq 5, 0 \leq j \leq 1\}$

因为 $(\overline{xy})^2 = 1$, 所以 $\overline{yx} = \overline{x}^{-1}\overline{y}^{-1} = \overline{x}^5\overline{y}$, 故对 $\forall 1 \leq j \leq 5$, 有

$$\overline{yx}^j = \overline{yx}\cdot\overline{x}^{j-1} = \overline{x}^5\overline{yx}\cdot\overline{x}^{j-2} = \overline{x}^{10}\overline{y}\cdot\overline{x}^{j-2} = \overline{x}^4\overline{y}\cdot\overline{x}^{j-2}$$

故不断进行上述过程, 可以将 G 中的元素写为 RHS 的形式, 进而断言得证, 故 $|G| \leq 12$, 且由 f 是满射知,f 是双射, 且保运算, 故 $G \simeq D_6$

Ex 证明 $< s, t \mid s^2, t^2, (st)^6 > \simeq D_6$

例 4.69 四元数群 Q_8

Q_8 的来源: $\mathbb{H} = \mathbb{R}\oplus\mathbb{R}i\oplus\mathbb{R}j\oplus\mathbb{R}k$, 有一组基 $\{1, i, j, k\}$ 满足 $i^2 = j^2 = k^2 = -1, ij = k, jk = i, ki = j$, 可以证明 $\mathbb{H}$ 是非交换结合环, 可除环, 记 $\mathbb{H}^\times = \mathbb{H}\backslash\{0\}$, 定义

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\} \leq \mathbb{H}^\times$$

则 Q_8 是 8 阶非 *Abel* 群

在 $Q_8, i^4 = 1 = j^4, i^2 = j^2 = -1, ji = -ij = i^3 j$, 令

$$G =< x, y \mid x^4 = 1, x^2 = y^2, yx = x^3 y >= \frac{F(x,y)}{N(x^4, x^2 y^{-2}, yxy^{-1}x^{-3})}$$

存在满射

$$f : G \longrightarrow Q_8$$
$$\overline{x} \longmapsto i$$
$$\overline{y} \longmapsto j$$

类似可以证明这是同构

评价 $D_4 = \Sigma(\square)$ 和 Q_8 都是 8 阶群, 但是 D_4 只有两个 4 阶元, 但 Q_8 有六个 4 阶元, 故它们不同构

评价 书上对 Q_8 的定义比较诡异, 较为反人类, 给当时的小伍造成了心理阴影

§4.8 有限生成 Abel 群

在本节中，约定群 A 的运算为加法，零元为 0，a 的负元为 $-a$，a 的幂次为 na

例 4.70 $(\mathbb{Z}, +), (\mathbb{Z}_n, +)$ 均为 Abel 群

定义 4.8.1（加法群的直和）设 $(A, +), (B, +)$ 为两个加法群，定义（约定）它们的直和为

$$A \oplus B = A \times B$$

零元为 $(0_A, 0_B)$

例 4.71 $\forall n \geq 1$，定义

$$\mathbb{Z}^n = \mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z} = \left\{ \begin{pmatrix} a_1 & \cdots & a_n \end{pmatrix}^T \middle| a_i \in \mathbb{Z} \right\}$$

零元定义为 $(0, \cdots, 0)^T$，负元定义为每个分量的负元

Fact $\mathbb{Z}^n$ 由 $\boldsymbol{e}_1, \cdots, \boldsymbol{e}_n$ 生成，其中 $\boldsymbol{e}_i$ 为第 i 个元素为 1 的单位向量. 即 $\forall \boldsymbol{v} \in \mathbb{Z}^n$ 可写成 $\boldsymbol{e}_1, \cdots, \boldsymbol{e}_n$ 的整线性组合

$$\begin{pmatrix} a_1 & \cdots & a_n \end{pmatrix}^T = \sum_{i=1}^{n} a_i \boldsymbol{e}_i$$

定义 4.8.2（有限基）对于加法群 A，称 $S \subseteq A, |S| < +\infty$ 为有限基，若

1. S 生成 A，即 $\forall a \in A, \exists a_i, 1 \leq i \leq n \in \mathbb{Z}, \text{s.t. } a = a_1 s_1 + \cdots + a_n s_n, a_i \in \mathbb{Z}, s_i \in S$
2. S 是 $\mathbb{Z}$-线性无关的，即 $\forall s_1, \cdots, s_n \in S$，若 $0_A = a_1 s_1 + \cdots + a_n s_n, a_i \in \mathbb{Z}$，则 $\forall i, a_i = 0$

例 4.72 并非所有加法群都有基！考虑 $(\mathbb{Z}_n, +)$，则 $\forall \overline{a} \in \mathbb{Z}_n, n\overline{a} = 0$，故 $\{\overline{a}\}$ 自身 $\mathbb{Z}$-线性相关

Fact $\{\boldsymbol{e}_1, \cdots, \boldsymbol{e}_n\}$ 是 $\mathbb{Z}^n$ 的一组基

命题 4.8.1 A 有有限基 $\iff \exists n \in \mathbb{N}, \text{s.t. } A \simeq \mathbb{Z}^n$

证明 ($\Longleftarrow$) 设有同构 $\theta : A \to \mathbb{Z}^n$，则

$$\{\theta^{-1}(\boldsymbol{e}_1), \cdots, \theta^{-1}(\boldsymbol{e}_n)\}$$

是 A 的一组基

($\Longrightarrow$) 设 A 有基 $S = \{s_1, \cdots, s_n\}$，考虑映射

$$\begin{aligned} \theta : \mathbb{Z}^n &\longrightarrow A \\ \begin{pmatrix} a_1 & \cdots & a_n \end{pmatrix}^T &\longmapsto \sum_{i=1}^{n} a_i s_i \end{aligned}$$

可以验证它是群同构 □

定义 4.8.3（秩）若 $A \simeq \mathbb{Z}^n$，则称 A 为秩 n 的自由 Abel 群

评价 区分与自由群的概念，“秩 n 的自由 *Abel* 群”是一个新概念

Ex 证明 $\mathbb{Z}^n \simeq < x_1, \cdots, x_n \mid x_i x_j = x_j x_i, \forall i \neq j >$

目标：分类有限生成的 Abel 群（有限生成即 $\exists S \subseteq A, |S| < +\infty, S$ 生成 A）

Fact 对于有限生成 Abel 群 A，一定存在正整数 n，使得 A 同构于 $\mathbb{Z}^n$ 的某个商群，即 $\exists K \leq \mathbb{Z}^n, \text{s.t.}$

$$A \simeq \mathbb{Z}^n / K$$

证明 设 $S = \{s_1, \cdots, s_n\}$ 为 A 的一个生成元集合，考虑满射

$$\begin{aligned} \phi : \mathbb{Z}^n &\longrightarrow A = (S) \\ \begin{pmatrix} a_1 & \cdots & a_n \end{pmatrix}^T &\longmapsto \sum_{i=1}^{n} a_i s_i \end{aligned}$$

由同态基本定理，$\mathbb{Z}^n / \mathrm{Ker}\phi \simeq A$ □

评价 注意区分有限生成和有限基这两个概念，如 $\mathbb{Z}_n$ 是有限生成的，它有生成元 $\{\overline{1}\}$，但是它却没有有限基（上面论述过了）

Fact 设 $K \leq \mathbb{Z}^n$，则 K 是有限生成的

证明 对 n 进行归纳

- $n = 1$ 时，$K \leq \mathbb{Z} \Longrightarrow K = m\mathbb{Z}, m \geq 0$
- $n = 2$ 时，设 $K \leq \mathbb{Z} \oplus \mathbb{Z} = \mathbb{Z}\boldsymbol{e}_1 \oplus \mathbb{Z}\boldsymbol{e}_2$，其中

$$\mathbb{Z}\boldsymbol{e}_1 = \{(n, 0) | n \in \mathbb{Z}\}, \quad \mathbb{Z}\boldsymbol{e}_2 = \{(0, n) | n \in \mathbb{Z}\}$$

因为 $(K\cap\mathbb{Z}\boldsymbol{e}_1)\leq\mathbb{Z}\boldsymbol{e}_1\simeq\mathbb{Z}$，因此 $K\cap\mathbb{Z}\boldsymbol{e}_1$ 是有限生成的，由第二同态定理

$$K/(K\cap\mathbb{Z}\boldsymbol{e}_1)\simeq(K+\mathbb{Z}\boldsymbol{e}_1)/\mathbb{Z}\boldsymbol{e}_1\leq\mathbb{Z}^2/\mathbb{Z}\boldsymbol{e}_1\simeq\mathbb{Z}$$

所以 $K/(K\cap\mathbb{Z}\boldsymbol{e}_1)$ 是有限生成的，由下面的练习即可证明 K 是有限生成的

- 对于一般的 n，由数学归纳法约化到 $n=2$ 的情形（小伍：我就不证了） □

Ex 假设 $N\leq G,N$ 是有限生成的，G/N 也是有限生成的，则 G 是有限生成的

约定记号

$$M_{n\times m}(\mathbb{Z})=\left\{\left(a_{ij}\right)_{n\times m}\middle|a_{ij}\in\mathbb{Z},1\leq i\leq n,1\leq j\leq m\right\}$$

Fact 给定 $A\in M_{n\times m}(\mathbb{Z})$

$$\begin{aligned}\phi_A:\mathbb{Z}^m&\longrightarrow\mathbb{Z}^n\\\boldsymbol{v}&\longmapsto A\boldsymbol{v}\end{aligned}$$

是 *Abel* 群同态，也称为 $\mathbb{Z}$-线性映射，$\phi_A(\boldsymbol{e}_i^{(m)})$ 为 A 的第 i 列

Fact 任意群同态 $\theta:\mathbb{Z}^m\to\mathbb{Z}^n$ 都形如 ϕ_A

证明 考虑

$$A=\begin{pmatrix}\theta(\boldsymbol{e}_1)&\cdots&\theta(\boldsymbol{e}_m)\end{pmatrix}$$

可以验证 $\theta=\phi_A$ □

综上，我们将上述事实总结为如下命题

命题 4.8.2 存在双射

$$\begin{aligned}M_{n\times m}(\mathbb{Z})&\longrightarrow\mathrm{Hom}(\mathbb{Z}^m,\mathbb{Z}^n)\\A&\longmapsto\phi_A\end{aligned}$$

Fact 给定 $B_{p\times n},A_{n\times m}$，有复合同态

$$\mathbb{Z}^m\xrightarrow{\phi_A}\mathbb{Z}^n\xrightarrow{\phi_B}\mathbb{Z}^p$$

$\phi_B\circ\phi_A=\phi_{BA}$，即同态的复合与矩阵乘法一一对应

命题 4.8.3 若 $\mathbb{Z}^n\simeq\mathbb{Z}^m$，则 $n=m$，即自由 Abel 群的秩的定义4.8.3是合理的

证明 存在 $B\in M_{m\times n}(\mathbb{Z}),A\in M_{n\times m}(\mathbb{Z})$，使得如下群同构成立

$$\phi_B:\mathbb{Z}^n\longrightarrow\mathbb{Z}^m\quad\phi_A:\mathbb{Z}^m\longrightarrow\mathbb{Z}^n$$

由群同构知 $\phi_{AB}=\phi_A\circ\phi_B=\mathrm{Id}_{\mathbb{Z}^n}$，故 $AB=I_n$，同理 $BA=I_m$，则

$$n=\mathrm{tr}(AB)=\mathrm{tr}(BA)=m$$

□

定义 4.8.4（余核）设 $A \in M_{n\times m}(\mathbb{Z}), \phi_A : \mathbb{Z}^m \to \mathbb{Z}^n, \mathrm{Im}(\phi_A) \leq \mathbb{Z}^n$，称

$$\mathrm{Coker}(\phi_A) \overset{\text{def}}{=} \mathbb{Z}^n/\mathrm{Im}(\phi_A)$$

为 ϕ_A 的余核；更一般地，若 $f : A \to B$ 是 *Abel* 群之间的同态，称商群 $B/\mathrm{Im}(f)$ 为 f 的余核，记为 $\mathrm{Coker}(f)$

评价 ϕ_A 是满射 $\iff \mathrm{Coker}(\phi_A) = \{0\}$ 是平凡的

Key Fact 有限生成的 *Abel* 群 G 均同构于 $\mathrm{Coker}(\phi_A)$，其中 A 是某个系数为整数的矩阵

证明 因为 G 同构于 $\mathbb{Z}^n$ 的某个商群，即 $G \simeq \mathbb{Z}^n/K$，且 K 有限生成，假设由 $\{\boldsymbol{v}_1, \cdots, \boldsymbol{v}_m\}$ 生成，令 $A = \begin{pmatrix} \boldsymbol{v}_1 & \cdots & \boldsymbol{v}_m \end{pmatrix}_{n\times m}$，则

$$\begin{aligned} \phi_A : \mathbb{Z}^m &\longrightarrow \mathbb{Z}^n \\ \boldsymbol{e}_i &\longmapsto \boldsymbol{v}_i \end{aligned}$$

因此 $\mathrm{Im}\phi_A = K$，故 $G \simeq \mathbb{Z}^n/K = \mathrm{Coker}(\phi_A)$ □

定义 4.8.5（可逆整方阵）

$$\begin{aligned} \mathrm{GL}_n(\mathbb{Z}) &\overset{\text{def}}{=} \{A \in M_n(\mathbb{Z}) | \exists B \in M_n(\mathbb{Z}), \text{s.t. } AB = I_n = BA\} \\ &= \{A \in M_n(\mathbb{Z}) | \det(A) = \pm 1\} \end{aligned}$$

Ex $A \in M_n(\mathbb{Z})$，则 $A \in \mathrm{GL}_n(\mathbb{Z}) \iff \phi_A : \mathbb{Z}^n \to \mathbb{Z}^n$ 是群同构

评价 由练习知 $\mathrm{GL}_n(\mathbb{Z}) \simeq \mathrm{Aut}(\mathbb{Z}^n)$，但是 $\mathrm{GL}_n(\mathbb{Z})$ 比较神秘，因为整系数方阵不能打洞

评价 小伍：我的品味不偏

定义 4.8.6（$\mathbb{Z}$-相抵）设 $A, B \in M_{n\times m}(\mathbb{Z})$，称 A, B $\mathbb{Z}$-相抵，若

$$B = PAQ$$

其中 $P \in \mathrm{GL}_n(\mathbb{Z}), Q \in \mathrm{GL}_m$，容易验证 $\mathbb{Z}$-相抵是 $M_{n\times m}(\mathbb{Z})$ 上的等价关系

Key Fact 若 A, B 相抵，则 $\mathrm{Coker}(\phi_A) \simeq \mathrm{Coker}(\phi_B)$

证明 由相抵可设 $B = P^{-1}AQ, P \in \mathrm{GL}_n(\mathbb{Z}), Q \in \mathrm{GL}_m(\mathbb{Z})$，则下面的（左半边）图交换，即 $\phi_A \circ \phi_Q = \phi_P \circ \phi_B$

$$\begin{array}{ccccc} \mathbb{Z}^m & \xrightarrow{\phi_A} & \mathbb{Z}^n & \xrightarrow{\text{can}} & \mathrm{Coker}(\phi_A) \\ \uparrow{\scriptstyle \phi_Q} & & \uparrow{\scriptstyle \phi_P} & & \uparrow{\scriptstyle \Phi_P} \\ \mathbb{Z}^m & \xrightarrow{\phi_B} & \mathbb{Z}^n & \xrightarrow{\text{can}} & \mathrm{Coker}(\phi_B) \end{array}$$

考虑映射

$$\Phi_P : \mathrm{Coker}(\phi_B) \longrightarrow \mathrm{Coker}(\phi_A)$$
$$\overline{\boldsymbol{v}} \longmapsto \overline{\phi_P(\boldsymbol{v})}$$

补充验证 Φ_P 的良定性：假设 $\overline{\boldsymbol{v}} = \overline{\boldsymbol{v}}'$，则 $\boldsymbol{v} - \boldsymbol{v}' \in \mathrm{Im}(\phi_B)$，因此 $\exists \boldsymbol{\mu} \in \mathbb{Z}^m, \text{s.t. } \phi_B(\boldsymbol{\mu}) = \boldsymbol{v} - \boldsymbol{v}'$，所以

$$\phi_P(\boldsymbol{v} - \boldsymbol{v}') = \phi_P \circ \phi_B(\boldsymbol{\mu}) = \phi_A \circ \phi_Q(\boldsymbol{\mu}) \in \mathrm{Im}(\phi_A)$$

所以 $\Phi_P(\overline{\boldsymbol{v}} - \overline{\boldsymbol{v}}') = \overline{\phi_P(\overline{\boldsymbol{v}} - \overline{\boldsymbol{v}}')} = \overline{\boldsymbol{0}}$，故 $\Phi_P(\overline{\boldsymbol{v}}) = \Phi_P(\overline{\boldsymbol{v}}')$

Ex 验证 Φ_P 是群同构

□

定理 4.8.1（Smith 标准型）设 $A \in M_{n\times m}(\mathbb{Z})$，则 A $\mathbb{Z}$-相抵于，即 $\exists P \in \mathrm{GL}_n(\mathbb{Z}), Q \in \mathrm{GL}_m(\mathbb{Z}), \text{s.t.}$

$$P^{-1}AQ = \begin{pmatrix} D & O \\ O & O \end{pmatrix}$$

其中 $D = \mathrm{diag}(d_1, \cdots, d_r), 1 \le d_1 \mid d_2 \mid \cdots \mid d_r, r = \mathrm{rank}(A)$，称 B 为 A 的 Smith 标准型

证明 考虑行/列变换

1. 互换行/列
2. 第 i 行乘以 $a \in \mathbb{Z}$ 加到第 j 行上，第 i 行不变
3. 行/列乘以 ± 1

***Claim*:** $A \sim \begin{pmatrix} d_1 & O \\ O & A' \end{pmatrix}$，且 $d_1 \mid A$ 的所有分量

（证明过于复杂，掌握算法即可）最后由数学归纳法即证 □

例 4.73 设 $\mathbb{Z}^2$ 中 $\begin{pmatrix} 2 & 6 \end{pmatrix}^T, \begin{pmatrix} 4 & 5 \end{pmatrix}^T$ 生成的子群为 K，则 $|\mathbb{Z}^2/K| = ?$

将 $A = \begin{pmatrix} 2 & 4 \\ 6 & 5 \end{pmatrix}$ 化为 Smith 标准型

$$\begin{pmatrix} 2 & 4 \\ 6 & 5 \end{pmatrix} \sim \begin{pmatrix} 2 & 4 \\ 0 & -7 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 \\ 0 & 7 \end{pmatrix} \sim \begin{pmatrix} 2 & 7 \\ 0 & 7 \end{pmatrix} \sim$$
$$\begin{pmatrix} 2 & 7 \\ 0 & 7 \end{pmatrix} \sim \begin{pmatrix} 2 & 1 \\ 0 & 7 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 \\ 7 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & 14 \end{pmatrix} = B$$

实际上 $K = \mathrm{Im}(\phi_A)$，所以

$$\mathbb{Z}^2/K = \mathrm{Coker}(\phi_A) \simeq \mathrm{Coker}(\phi_B) = \mathbb{Z}^2 \Big/ \left\{ \begin{pmatrix} a \\ 14b \end{pmatrix} \middle| a, b \in \mathbb{Z} \right\}$$
$$\simeq \mathbb{Z}^2/\mathbb{Z} \oplus (14\mathbb{Z}) \simeq \mathbb{Z}/\mathbb{Z} \oplus (\mathbb{Z}/14\mathbb{Z}) = \{0\} \times \mathbb{Z}_{14}$$

所以 $|\mathbb{Z}^2/K| = 14$（第二行由下面的练习保证，讲到这里的时候下课了）

回顾关键事实

Key Fact 有限生成的 Abel 群 G 均同构于 $\mathrm{Coker}(\phi_A)$，其中 A 是某个矩阵

假设 $B=\mathrm{diag}(d_1,\cdots,d_r,0,\cdots,0)$ 是 A 的 Smith 标准型，考虑

$$\begin{aligned}\phi_B:\mathbb{Z}^m &\longrightarrow \mathbb{Z}^n\\ \boldsymbol{e}_i &\longmapsto d_i\boldsymbol{e}_i,\quad 1\le i\le r\\ \boldsymbol{e}_i &\longmapsto \boldsymbol{0},\quad i>r\end{aligned}$$

则

$$\begin{aligned}\mathrm{Im}(\phi_B)&=\left\{\begin{pmatrix}d_1a_1 & \cdots & d_ra_r & 0 & \cdots & 0\end{pmatrix}\middle| a_i\in\mathbb{Z}\right\}\\ &=d_1\mathbb{Z}_1\times\cdots\times d_r\mathbb{Z}\times 0\mathbb{Z}\times\cdots\times 0\mathbb{Z}\subset\mathbb{Z}^n\end{aligned}$$

进而由下面的练习知

$$\mathrm{Coker}(\phi_A)\simeq\mathrm{Coker}(\phi_B)\simeq(\mathbb{Z}_{d_1}\oplus\cdots\oplus\mathbb{Z}_{d_r})\oplus\mathbb{Z}^{n-r}$$

Ex $G_1,\cdots,G_n$ 是群，$N_1\lhd G_1,\cdots,N_n\lhd G_n$，则

1. $(N_1\times\cdots\times N_n)\lhd(G_1\times\cdots\times G_n)$
2. $\frac{(G_1\times\cdots\times G_n)}{(N_1\times\cdots\times G_n)}\simeq(G_1/N_1)\times\cdots\times(G_n/N_n)$

总结如下

定理 4.8.2（有限生成 Abel 群的结构定理）任意有限生成的 Abel 群 G，则

$$G\simeq(\mathbb{Z}_{d_1}\oplus\cdots\oplus\mathbb{Z}_{d_r})\oplus\mathbb{Z}^s$$

其中 $s\ge 0, 1\mid d_1\mid\cdots\mid d_r$，特别地若 $|G|<+\infty$，则

$$G\simeq\mathbb{Z}_{d_1}\oplus\cdots\oplus\mathbb{Z}_{d_r}$$

其中 $1\mid d_1\mid\cdots\mid d_r$

证明

Step 1. $\exists A\in M_{n\times m}(\mathbb{Z})$, s.t. $G\simeq\mathrm{Coker}(\phi_A)$

Step 2. $A\sim B$，其中 B 为 Smith 标准型，$\mathrm{Coker}(\phi_B)$ 可算！ □

推论 4.8.1 设 $A\in M_n(\mathbb{Z}),\det(A)\neq 0$，则 $|\mathrm{Coker}(\phi_A)|<+\infty$，且 $|\mathrm{Coker}(\phi_A)|=|\det(A)|$

证明 A 有 Smith 标准型 $B=\mathrm{diag}(d_1,\cdots,d_n)$，且 $|\det(A)|=|\det(B)|=d_1\cdots d_n$，且

$$\begin{aligned}\mathrm{Coker}(\phi_A)&\simeq\mathrm{Coker}(\phi_B)\\ &\simeq\mathbb{Z}_{d_1}\oplus\cdots\oplus\mathbb{Z}_{d_n}\end{aligned}$$

故 $|\mathrm{Coker}(\phi_A)| = d_1 \cdots d_n = |\det(A)|$ □

推论 4.8.2 设 $K \leq \mathbb{Z}^n$（因此 K 是有限生成的），则

(1) $\exists \mathbb{Z}^n$ 的基 $\{\boldsymbol{v}_1, \cdots, \boldsymbol{v}_n\}$ 和 $d_1 \mid \cdots \mid d_r, r \leq n$，使得 K 恰以 $d_1\boldsymbol{v}_1, \cdots, d_r\boldsymbol{v}_r$ 为基，因此 K 也是有限生成自由 Abel 群，且 $\mathrm{rank}(K) = r \leq n$

(2) $\mathbb{Z}^n/K \simeq \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_r} \oplus \mathbb{Z}^{n-r}$

证明 (1). 因为 K 是有限生成的，设生成元为 $\xi_1, \cdots, \xi_m$，考虑

$$A = \begin{pmatrix} \xi_1 & \cdots & \xi_m \end{pmatrix}_{n \times m}$$

考虑映射

$$\begin{aligned} \phi_A : \mathbb{Z}^m &\longrightarrow \mathbb{Z}^n \\ \boldsymbol{e}_i &\longmapsto \xi_i (A \text{ 的第 } i \text{ 列}) \end{aligned}$$

所以 $\exists A \in M_{n\times m}(\mathbb{Z}), \text{s.t. } K = \mathrm{Im}(\phi_A)$，设 $B = P^{-1}AQ$，其中 B 为 A 的 Smith 标准型

$$\begin{array}{ccc} \mathbb{Z}^m & \xrightarrow{\phi_A} & \mathbb{Z}^n \\ {\scriptstyle \phi_Q}\uparrow & & \uparrow{\scriptstyle \phi_P} \\ \mathbb{Z}^m & \xrightarrow{\phi_B} & \mathbb{Z}^n \end{array}$$

取 $\mathbb{Z}^n$ 的标准正交基 $\{\boldsymbol{e}_1, \cdots, \boldsymbol{e}_n\}$，则 $\{d_1\boldsymbol{e}_1, \cdots, d_r\boldsymbol{e}_r\}$ 为 $\mathrm{Im}(\phi_B)$ 的一组基，设 $P = \begin{pmatrix} \boldsymbol{v}_1 & \cdots & \boldsymbol{v}_n \end{pmatrix}$，由 B 可逆知 $\{\boldsymbol{v}_1, \cdots, \boldsymbol{v}_n\}$ 是 $\mathbb{Z}^n$ 的一组基，因为

$$\mathrm{Im}(\phi_A) = \phi_P(\mathrm{Im}\phi_B) =< \phi_P(d_1\boldsymbol{e}_1), \cdots, \phi_P(d_r\boldsymbol{e}_r) >=< d_1\boldsymbol{v}_1, \cdots, d_r\boldsymbol{v}_r >$$

因此 K 恰以 $\{d_1\boldsymbol{v}_1, \cdots, d_r\boldsymbol{v}_r\}$ 为基

(2). 是自然的推论 □

定义 4.8.7（扭子群） $(G, +)$ 中的有限阶元称为扭元 (torsion element)，定义 $(G, +)$ 的所有有限阶元构成的集合为 G 的扭子群（可以验证它确实是群），记为

$$t(G) = \{g \in G : g\text{有限阶}\} \leq G$$

若 G 没有扭元 (torsion free)，即 $t(G) = \{0_G\}$，称 G 为无扭群；若 $G = t(G)$，则称 G 为扭群

例 4.74 $(\mathbb{Z}, +), (\mathbb{Q}, +)$ 无扭；$\mathbb{Q}\backslash\mathbb{Z}$ 是扭群

Ex 有限生成的扭群是有限的

定理 4.8.3 设 G 是有限生成 Abel 群，则存在内直和分解

$$G = t(G) \oplus F$$

使得 F 是有限生成的自由 Abel 群，称为 $t(G)$ 的补；且 $|t(G)|<+\infty, t(G)\simeq \mathbb{Z}_{d_1}\oplus\cdots\oplus\mathbb{Z}_{d_r}$

证明 有群同构

$$\theta: G\simeq (\mathbb{Z}_{d_1}\oplus\cdots\oplus\mathbb{Z}_{d_r})\oplus\mathbb{Z}^s$$

记 $(\mathbb{Z}_{d_1}\oplus\cdots\oplus\mathbb{Z}_{d_r})\oplus\mathbb{Z}^s=R$，因为 $\mathbb{Z}^s$ 中除 0 外没有扭元，所以 $t(R)=(\mathbb{Z}_{d_1}\oplus\cdots\oplus\mathbb{Z}_{d_r})\oplus(0\mathbb{Z})^s$，因此存在内直和

$$R=t(R)\oplus F',\quad F'\simeq\mathbb{Z}^s$$

作用 θ^{-1} 得

$$G=t(G)\oplus\theta^{-1}(F')\overset{\text{def}}{=}t(G)\oplus F$$

□

评价 因为 $F\simeq G/t(G)$，故 F 不唯一，但同构意义下唯一

例 4.75 设 $G=\mathbb{Z}_2\times\mathbb{Z}$，则 $t(G)=\mathbb{Z}^2\times\{0\}=<(\overline{0},0),(\overline{1},0)>$，记

$$\begin{cases}F_1=\overline{0}\times\mathbb{Z}=\{(\overline{0},n)|n\in\mathbb{Z}\}\\ F_2=\{(\overline{n},n)|n\in\mathbb{Z}\}\end{cases}$$

Ex $t(G)$ 仅有这两个补！

推论 4.8.3 设 G 是无扭群且有限生成，则 G 是有限生成的自由 Abel 群

评价 有限生成是必须的，考虑 $\mathbb{Q}$

定义 4.8.8（有限生成 Abel 群的秩）设 G 是有限生成 Abel 群，定义 $\operatorname{rank}(G)=\operatorname{rank}(F)$

推论 4.8.4 设 G,H 为有限生成 Abel 群，则

$$G\simeq H\iff\begin{cases}t(G)\simeq t(H)\\ \operatorname{rank}(G)=\operatorname{rank}(H)\end{cases}$$

评价 $\operatorname{rank}(G)=\dim_{\mathbb{Q}}(\mathbb{Q}\otimes_{\mathbb{Z}}G)$，见交换代数

定义 4.8.9（初等因子与不变因子）设 G 是有限 Abel 群，由定理 4.8.2 知

$$G\simeq\mathbb{Z}_{d_1}\times\cdots\times\mathbb{Z}_{d_r}$$

我们称 $\{d_1,\cdots,d_r\}$ 为 G 的不变因子，设 d_i 有素因子分解 $d_i=p_1^{s_{i1}}\cdots p_l^{s_{il}}$，其中 $1\le i\le r$，由中

国剩余定理知 $\mathbb{Z}_{d_i} \simeq \mathbb{Z}_{p_1^{s_{i1}}} \times \cdots \times \mathbb{Z}_{p_l^{s_{il}}}$，按素因子重新排序可得

$$\begin{aligned} G &\simeq \left(\mathbb{Z}_{p_1^{s_{11}}} \oplus \cdots \oplus \mathbb{Z}_{p_l^{s_{1l}}}\right) \oplus \cdots \oplus \left(\mathbb{Z}_{p_1^{s_{r1}}} \oplus \cdots \oplus \mathbb{Z}_{p_l^{s_{rl}}}\right) \\ &\simeq \left(\mathbb{Z}_{p_1^{s_{11}}} \oplus \cdots \oplus \mathbb{Z}_{p_1^{s_{r1}}}\right) \oplus \cdots \oplus \left(\mathbb{Z}_{p_l^{s_{rl}}} \oplus \cdots \oplus \mathbb{Z}_{p_l^{s_{rl}}}\right) \\ &\overset{\text{def}}{=} B_{p_1} \oplus \cdots \oplus B_{p_l} \end{aligned}$$

其中 $B_{p_i} = \mathbb{Z}_{p_i^{s_{1i}}} \times \cdots \times \mathbb{Z}_{p_i^{s_{ri}}}$ 为 G 的 p_i-*Sylow* 子群，我们称

$$\begin{Bmatrix} p_1^{s_{11}} & p_2^{s_{12}} & \cdots & p_l^{s_{1l}} \\ p_1^{s_{21}} & p_2^{s_{22}} & \cdots & p_l^{s_{2l}} \\ \vdots & \vdots & & \vdots \\ p_1^{s_{r1}} & p_2^{s_{r2}} & \cdots & p_l^{s_{rl}} \end{Bmatrix}$$

为 G 的初等因子，由 $d_1 \mid \cdots \mid d_r$ 知，$s_{1i} \le s_{2i} \le \cdots \le s_{ri}, \forall 1 \le i \le l$

Fact 设 G 是 Abel p-群，若

$$\begin{cases} B \simeq \mathbb{Z}_{p^{s_1}} \times \cdots \times \mathbb{Z}_{p^{s_l}}, & s_1 \le \cdots \le s_l \\ B \simeq \mathbb{Z}_{p^{t_1}} \times \cdots \times \mathbb{Z}_{p^{t_l}}, & t_1 \le \cdots \le t_r \end{cases}$$

则 $r = l, s_1 = t_1, \cdots, s_r = t_r$

证明 考虑

$$B \supseteq pB \supseteq p^2B \supseteq \cdots \supseteq p^mB = 0$$

因为 $p^kB/p^{k+1}B$ 是 $\mathbb{F}_p$-线性空间，且

$$\dim_{\mathbb{F}_p}(p^kB/p^{k+1}B) = \#\{s_i : s_k \ge k, 1 \le i \le l\}$$

□

评价 初等因子决定不变因子；反之不变因子决定初等因子

定理 4.8.4（唯一性）设

$$G \simeq \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_r}$$

其中 $d_1 \mid \cdots \mid d_r$，则 $d_1, \cdots, d_r$ 由 G 唯一决定

证明 大家自己去琢磨一下 □

Ex 分类 1500 阶 Abel 群 G

解 因为 $1500 = 2^2 3^1 5^3$，在同构意义下讨论 G 的 Sylow-p_i 子群

Sylow-2 子群：$\mathbb{Z}_2^2$ 或 $\mathbb{Z}_2 \oplus \mathbb{Z}_2$，共 2 种

Sylow-3 子群：$\mathbb{Z}_3$，共 1 种

Sylow-5 子群：$\mathbb{Z}_5^3$ 或 $\mathbb{Z}_5^2 \oplus \mathbb{Z}_5$ 或 $\mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$，共 3 种

因此 1500 阶群 G 共有 $3 \times 2 = 6$ 种 □

§4.9 思考题

本小节是在小伍所谓的“垃圾时间”讲的.

例 4.76 设 $D_\infty =< s,t \mid s^2 = t^2 = 1 >= F(s,t)/N(s^2,t^2)$，记 $s = \overline{s} = sN, t = \overline{t} = tN$，证明 st 无穷阶

证明 回忆 $D_{2n} =< x,y \mid x^n = 1, y^2 = 1, (xy)^2 = 1 >$，$|D_{2n}| = 2n, \mathrm{Ord}(x) = n$，若 $(st)^n = 1$，考虑

$$\begin{aligned} \theta : \{s,t\} &\longrightarrow D_{2(n+1)} \\ t &\longmapsto y \\ s &\longmapsto xy \end{aligned}$$

由命题 4.7.2，因为 $\theta(t), \theta(s)$ 满足 G 中关系 $s^2 = t^2 = 1$，故 θ 可延拓至群同态 $\tilde{\theta} : D_\infty \to D_{2(n+1)}$，所以 $\tilde{\theta}(st) = x$，但是与 x 的阶为 $n+1$ 矛盾! □

定义 4.9.1（群作用在群上）设 G, N 是群，若有群同态 $G \xrightarrow{\rho} \mathrm{Aut}(N)$，则称 G 作用在群 N 上

Fact $(N, \phi) \iff$ 存在映射

$$\begin{aligned} \phi : G \times N &\longrightarrow N \\ (g,n) &\longmapsto g.n = \rho(g)(n) \end{aligned}$$

满足

(1) $g'(g.n) = (g'g).n$

(2) $(1_G).n = n$

(3) $g.(nn') = (g.n)(g.n'), n, n' \in N, g \in G$

例 4.77（共轭作用）设 G 是群，$N \lhd G, H \leq G$，则 H 作用于子群 N

$$h.n = hnh^{-1} \in N$$

定义 4.9.2（半直积）设群 H 作用于子群 N，即存在群同态 $\rho : H \to \mathrm{Aut}(N)$，群 $N \rtimes_\rho H$ 称为 ρ 对应的半直积（常常略去 $\rtimes_\rho$ 中的 ρ）

(1) 作为集合，$N \rtimes_\rho H = N \times H$

(2) 二元运算定义为

$$\begin{aligned} (n,h)(n',h') &= (n(h.n'), hh') \\ &= (n\rho(h)(n'), hh') \end{aligned}$$

通过半直积可以构造出很多新的群

定理 4.9.1 设 $N \lhd G, H \leq G, N \cap H = \{1_G\}, G = NH$，设 $\rho : H \to \mathrm{Aut}(N)$ 为共轭作用，即 $\rho(h) = (n \mapsto hnh^{-1})$，则有群同构

$$\begin{aligned} N \rtimes_\rho H &\xrightarrow{\sim} G \\ (n, h) &\longmapsto nh \end{aligned}$$

例 4.78 $A_3 \lhd S_3$，设 $H = \{\mathrm{Id}, (12)\}$，则定理 4.9.1 中的共轭作用具体为

$$\begin{aligned} \rho : H &\xrightarrow{\sim} \mathrm{Aut}(A_3) \\ \mathrm{Id} &\longmapsto \mathrm{Id} \\ (12) &\longmapsto \text{求逆} \end{aligned}$$

由定理 4.9.1 ，$S_3 \simeq A_3 \rtimes H \simeq C_3 \rtimes C_2$，即 S_3 是循环群的半直积

例 4.79 $K_4 = \{\mathrm{Id}, (12)(34), (13)(24), (14)(23)\} \lhd A_4$，设 $H = \{\mathrm{Id}, (123), (132)\}$，可以验证 $A_4 = K_4 H$，由定理 4.9.1 知，$K_4 \rtimes_\rho H \simeq A_4$

Ex $D_8 =< a, b \mid a^4 = 1 = b^2 = (ab)^2 >$，以下考虑共轭作用

1. 取 $N_1 =< a >, H_1 =< b >$，算 $\rho_1 : H_1 \to \mathrm{Aut}(N_1)$
2. 取 $N_2 =< a^2, b >, H_2 =< ab >$，算 $\rho_2 : H_2 \to \mathrm{Aut}(N_2)$

第五章 Galois 理论

§5.1 Galois 扩张

Recall：给定域扩张 K/k（自然视 $k \overset{\text{子域}}{\subseteq} K$，若为 $\theta: k \hookrightarrow K$，则此时将 k 与 $\theta(k)$ 等同）

1. K 成为 k-线性空间

$$\lambda \boldsymbol{v} = \lambda \cdot \boldsymbol{v}, \quad \lambda \in k, \boldsymbol{v} \in K$$

并记域扩张的维数 $\dim_k K = [K:k]$

2. K/k 的 Galois 群

$$\mathrm{Gal}(K/k) \overset{\text{def}}{=} \mathrm{Aut}(K/k) = \{\sigma \in \mathrm{Aut}(K) : \sigma|_k = \mathrm{Id}_k, \text{i.e } \theta(\lambda) = \lambda, \forall \lambda \in K\}$$

因此 $\sigma \in \mathrm{Gal}(K/k)$ 保“系数”，且我们有 $\mathrm{Gal}(K/k) \leq \mathrm{Aut}(K)$

引理 5.1.1 若 K/k 为有限维域扩张，即 $\dim_k K < +\infty$，则

$$|\mathrm{Gal}(K/k)| \leq \dim_k K < +\infty$$

定义 5.1.1（分裂域）称 $K = (k, f(x))$ 为 $f(x) \in k[x]$ 的分裂域，若

(1) $f(x)$ 在 K 上分裂 Spilt，即

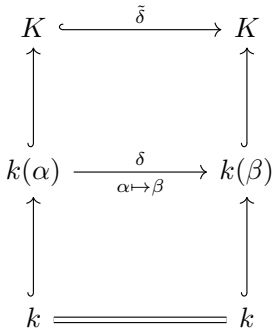
$$f(x) = (x - a_1) \cdots (x - a_n) \quad \text{in } K[x]$$

(2) K 是包含 $k, a_1, \cdots, a_n$ 的最小域，即 $K = k(a_1, \cdots, a_n)$

Key Fact $f(x) \in k[x]$ 可分，$K = (k, f(x))$，则

$$|\mathrm{Gal}(K/k)| = \dim_k K < +\infty$$

证明 对 $\dim_k K$ 归纳，设 $\alpha \in K/k, \alpha$ 在 $k[x]$ 上的最小多项式为 $g(x)$，任取 $\beta \in \mathrm{Root}_K(g(x))$，则存在唯一的延拓 $\delta: k(\alpha) \to k(\beta), \alpha \mapsto \beta$



由维数公式

$$\dim_k K = \dim_k k(\alpha) \cdot \dim_{k(\alpha)} K$$

若 f 可分，则这样的 δ 共有 $|\mathrm{Root}_k(g(x))| = \deg g(x) = \dim_k(k(\alpha))$ 个，因为 $\dim_{k(\alpha)} K < \dim_k K$，由 $f(x) \in k[x]$ 可分知，$f(x) \in k(\alpha)[x]$ 可分，由数学归纳法，对于每个 δ，共有 $\dim_{k(\alpha)} K$ 个延拓，故 $|\mathrm{Gal}(K/k)| = \dim_k k(\alpha) \cdot \dim_{k(\alpha)} K = \dim_k K$ □

例 5.1 考虑 $\mathbb{Q}(\sqrt[3]{2}/\mathbb{Q}), \dim_{\mathbb{Q}}(\mathbb{Q}\sqrt[3]{2}) = 3$，但 $\mathrm{Gal}(\mathbb{Q}\sqrt[3]{2}/\mathbb{Q}) = \{\mathrm{Id}\}$，

定义 5.1.2（不动子域）设 $G \leq \mathrm{Aut}(K)$，则有群作用 $G \curvearrowright K$

$$\begin{aligned} G \times K &\longrightarrow K \\ (\sigma, \boldsymbol{v}) &\longmapsto \sigma.\boldsymbol{v} = \sigma(\boldsymbol{v}) \end{aligned}$$

K 关于 G 的不动子域为

$$K^G = \{\boldsymbol{v} \in K : \sigma(\boldsymbol{v}) = \boldsymbol{v}, \forall \sigma \in G\}$$

只需验证逆元存在性：对 $\forall \sigma \in G \leq \mathrm{Aut}(K)$，$\sigma(\boldsymbol{v}^{-1}) = \sigma(\boldsymbol{v})^{-1} = \boldsymbol{v}^{-1}$，故 K^G 确实是 K 的子域

Fact (1) 若 $H \leq G \leq \mathrm{Aut}(K)$，则

$$K^G \subseteq K^H \subseteq K = K^{\mathrm{Id}_K}$$

(2) 给定域扩张 K/k 以及群 $G \leq \mathrm{Gal}(K/k)$，则

$$k \subseteq K^G \subseteq K$$

称 K^G 为中间域

(3) 给定域扩张 K/k，在 (2) 中取 $G = \mathrm{Gal}(K/k)$，则

$$k \subseteq K^{\mathrm{Gal}(K/k)} = \{v \in K : \forall \sigma \in \mathrm{Gal}(K/k), \sigma(v) = v\} \subseteq K$$

(4) 取 $G \leq \mathrm{Aut}(K)$，考虑域扩张 K/K^G，则有

$$G \leq \mathrm{Gal}(K/K^G) = \{\sigma \in \mathrm{Aut}(K) : \sigma|_{K^G} = \mathrm{Id}_{K^G}\}$$

定理 5.1.1 若 $G \leq \mathrm{Aut}(K)$ 为有限子群，则

(1) $[K : K^G] = |G|$

(2) $G = \mathrm{Gal}(K/K^G)$

证明 记 $k = K^G$，设 $|G| = n, G = \{\sigma_1, \cdots, \sigma_n\}$

***Claim*:** $\dim_k K \leq n$

Proof Of Claim : 否则存在 $\{e_1, \cdots, e_{n+1}\} \subset K$，它们 k-线性无关. 考虑 $n \times (n+1)$ 阶矩阵

$$A = \begin{pmatrix} \sigma_1(e_1) & \sigma_1(e_2) & \cdots & \sigma_1(e_{n+1}) \\ \sigma_2(e_1) & \sigma_2(e_2) & \cdots & \sigma_2(e_{n+1}) \\ \vdots & \vdots & & \vdots \\ \sigma_n(e_1) & \sigma_n(e_2) & \cdots & \sigma_n(e_{n+1}) \end{pmatrix}$$

记 A 的解空间为 $V=\{\boldsymbol{v}\in K^{n+1}:A\boldsymbol{v}=0\}\subset K^{n+1}$（线性子空间），考虑群作用 $G\curvearrowright K^{n+1}$

$$\begin{aligned} G\times K^{n+1}&\longrightarrow K^{n+1}\\ \left(\sigma,(\lambda_1,\cdots,\lambda_{n+1})^T\right)&\longmapsto \sigma.\boldsymbol{v}=\left(\sigma(\lambda_1),\cdots,\sigma(\lambda_{n+1})\right)^T\end{aligned}$$

SubClaim：若 $\boldsymbol{v}\in V$，则对 $\forall\tau\in G,\tau.\boldsymbol{v}\in V$

对 $\forall\boldsymbol{v}=(\lambda_1,\cdots,\lambda_{n+1})^T\in V$，有

$$\sum_{i=1}^{n+1}\lambda_i\sigma_t(e_i)=0,1\le t\le n$$

对 $\forall\tau\in G$，两边同时作用 τ 得

$$0=\tau\left(\sum_{k=1}^{n+1}\lambda_k\sigma_t(e_k)\right)=\sum_{k=1}^{n+1}\tau(\lambda_k)\tau(\sigma_t(e_k))$$

对 $\forall 1\le s\le n$，取 $\sigma_t=\tau^{-1}\sigma_s$，则

$$\sum_{k=1}^{n+1}\tau(\lambda_k)\sigma_s(e_k)=0$$

取 $\boldsymbol{v}=(\lambda_1,\cdots,\lambda_{n+1})^T\in V$，使得 $\boldsymbol{v}$ 中的 0 分量最多，注意到 0 分量的个数 $<n-1$（否则不妨设 $\boldsymbol{v}'=(\lambda_1,0,\cdots,0)^T,\lambda_1\neq 0$，则由 $A\boldsymbol{v}'=0$ 知，$\lambda_1\sigma_1(e_1)=0_K$，故 $\sigma_1(e_1)=0_K\Longrightarrow e_1=0_K$，矛盾!）

不妨设 $\boldsymbol{v}=(\lambda_1,\lambda_2,\cdots,\lambda_{n+1})^T,\lambda_1,\lambda_2\neq 0$，其余 λ_i 要求零元素是 V 中最多，由 V 是线性空间，可不妨设 $\lambda_1=1$，又注意到 $\lambda_2,\cdots,\lambda_{n+1}$ 不全在 k 中，（否则由 $\boldsymbol{v}\in V,A\boldsymbol{v}=0$ 知，考虑 A 中 $\sigma_i=\mathrm{Id}$ 的那一行，$\lambda_1e_1+\cdots+\lambda_{n+1}e_{n+1}=0$，与它们线性无关矛盾!）

不妨设 $\lambda_2\notin k=K^G$，则 $\exists\tau\in G,\text{s.t. }\tau(\lambda_2)\neq\lambda_2$，故

$$0\neq\boldsymbol{v}-\tau.\boldsymbol{v}=(0,\lambda_2-\tau(\lambda_2),\cdots,\lambda_{n+1}-\tau(\lambda_{n+1}))^T\in V$$

若 λ_i 本来就为零，则 $\lambda_i-\tau(\lambda_i)=0$，若 $\lambda_i\neq 0$，则 $\lambda_i-\tau(\lambda_i)$ 有可能为零，但是第一个分量确定变为零，故 $\boldsymbol{v}-\tau.\boldsymbol{v}$ 的 0 分量更多，故矛盾!

因此断言得证，故

$$n=|G|\overset{\text{Fact(4)}}{\le}|\mathrm{Gal}(K/k)|\le\dim_k K\overset{\textbf{\textit{Claim}}}{\le}n$$

□

定理 5.1.2 若 K/k 是有限维域扩张，记 $G=\mathrm{Gal}(K/k)$，则以下等价 TFAE

(1) $k=K^G$

(2) $|G|=\dim_k K$

(3) $\forall\alpha\in K$，则 α 在 k 上的最小多项式无重根，且在 K 上分裂

(4) $K=(k,f(x)),f(x)\in k[x]$ 可分

此时我们称 K/k 为（有限维）Galois 扩张

评价 (3) 是 local 局部描述；(4) 是 global 整体描述

证明 (1) $\iff$ (2)：因为

$$\dim_k K = \dim_k(K^G)\cdot[K:K^G] = \dim_k K^G \cdot |G|$$

所以 $k = K^G \iff \dim_k K^G = 1 \iff |G| = \dim_k K$

(2) $\Longrightarrow$ (3)：对 $\forall \alpha \in K$，设它的最小多项式为 $g(x)$，因为

$$|G| = |\mathrm{Gal}(K/k)| \le |\mathrm{Root}_K\big(g(x)\big)|\cdot[K:k(\alpha)] \le \deg\big(g(x)\big)\cdot[K:k(\alpha)] = [K:k]$$

由 $|G| = [K:k]$ 知，上式全为等号，故 $|\mathrm{Root}_K\big(g(x)\big)| = \deg\big(g(x)\big)$，即 $g(x)$ 无重根

(3) $\Longrightarrow$ (4)：设 $K = k(\alpha_1,\cdots,\alpha_n), \alpha_i$ 的最小多项式为 $g_i(x)$，令 $f(x) = g_1(x)\cdots g_n(x)$，则 $f(x)$ 可分且 $K = (k, f(x))$ 为 $f(x)$ 的分裂域

(4) $\Longrightarrow$ (2)：这是刚刚证明的 KeyFact □

Ex 假设存在同构 $\delta: k \xrightarrow{\sim} k'$，若有域扩张 $K/k, K'/k'$，则 $|\delta$的延拓$| \le \dim_k K$

定理 5.1.3（绝对 Galois 双射 Absolute Galois Bijection）对任意域 K，存在双射

$$\begin{aligned}\{\text{有限群} G \le \mathrm{Aut}(K)\} &\xleftrightarrow{1:1} \{k \subseteq K : K/k\text{有限维Galois扩张}\}\\ G &\longmapsto K^G\\ \mathrm{Gal}(K/E) &\longmapsfrom E\end{aligned}$$

Ex 求 $K = \mathbb{Q}(\sqrt[3]{2})$ 的绝对 Galois 双射

定理 5.1.4（相对 Galois 双射 Relative Galois Bijection）设 K/k 是有限维 Galois 扩张，存在双射

$$\begin{aligned}\{\mathrm{Gal}(K/k)\text{的子群}\} &\xleftrightarrow{1:1} \{K/k\text{的中间域}\}\\ H &\longmapsto K^H\\ \mathrm{Gal}(K/E) &\longmapsfrom E\end{aligned}$$

评价 由定理5.1.2(3) 知，在 K/k 是有限维 Galois 扩张的前提下，K/E 总是有限维 Galois 扩张

Ex 考虑域扩张塔 $k \subseteq E \subseteq K$，则 K/E 是有限维 Galois 扩张（但是 E/k 不一定是 Galois 扩张，见下练习）

Ex 考虑域扩张塔 $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[3]{2},\omega) = (\mathbb{Q}, x^3-2)$，证明

1. $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$ 不是 Galois 扩张
2. $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[3]{2},\omega)$ 是 Galois 扩张

命题 5.1.1 设 K/k 是有限维 Galois 扩张，对于域扩张塔 $k \subseteq E \subseteq K$，则 E/k 是有限维 Galois 扩张 $\iff \forall \sigma \in \mathrm{Gal}(K/k), \sigma(E) = E$

证明 $(\Longrightarrow)$: E 是有限维 Galois 扩张，则 $\exists g(x) = (x-\beta_1)\cdots(x-\beta_m) \in k[x], \text{s.t. } E = (k, g(x)) = k(\beta_1, \cdots, \beta_m)$，对 $\forall \sigma \in \mathrm{Gal}(K/k)$，下面证明 $\sigma(\beta_i) \in E, \forall i$，考虑 β_1 即可，其余同理

对 $g(\beta_1) = 0_E$ 两边作用 σ，因为 σ 保(k 上的)系数，所以 $g(\sigma(\beta_1)) = 0_E$，故 $\sigma(\beta_1) \in \mathrm{Root}_E(g(x)) \subset E$，所以 $\sigma(E) \subseteq E$，且 $\dim_k \sigma(E) = \dim_k E$，故 $\sigma(E) = E$

$(\Longleftarrow)$: 对 $\forall \beta \in E$，设它在 k 上的最小多项式为 $g(x)$

***Claim*:** $g(x)$ 在 E 上分裂

Proof Of Claim : 由 $g(x)$ 在 K 上分裂知，在 $K[x]$ 上有 $g(x) = (x-\beta_1)\cdots(x-\beta_m)$，则对 $\forall \beta_i \in \mathrm{Root}_K(g(x))$，$\mathrm{Id}_k$ 有延拓

$$\begin{aligned} \delta_i : k(\beta) &\xrightarrow{\sim} k(\beta_i) \\ \beta &\longmapsto \beta_i \end{aligned}$$

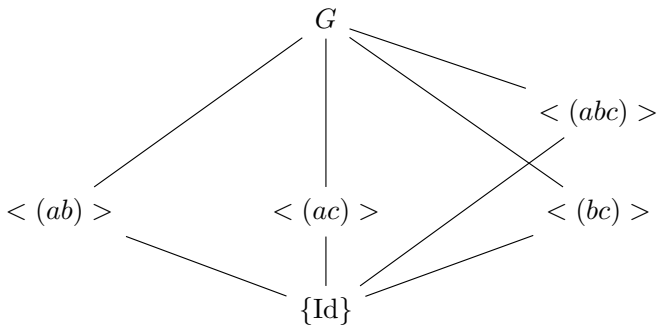
上面定义的 $\delta_i \in \mathrm{Gal}(K/k)$，故 $\beta_i = \delta_i(\beta) \in \sigma(E) = E$，故 $g(x) \in E$ 无重根，且在 E 上分裂，故 E/k 是有限维 Galois 扩张 □

评价 $\mathrm{Gal}(K/k)$ 中的元素保多项式的根

Ex 设 K/k 是有限维 Galois 扩张，$G = \mathrm{Gal}(K/k), g(x) \in k[x]$ 不可约，则群作用 $G \curvearrowright \mathrm{Root}_K(g(x))$ 可迁！

例 5.2 设 $K = \mathbb{Q}(\sqrt[3]{2}, \omega), K/\mathbb{Q}$ 是有限维 Galois 扩张，记 $G = \mathrm{Gal}(K/\mathbb{Q}) = \mathrm{Aut}(K)$，考虑群作用 $G \curvearrowright \mathrm{Root}_K(x^3-2) = \{\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2\} \overset{\text{记为}}{=} \{a, b, c\}$ 则它对应的群同态（实际上为群同构）

$$\rho : G \overset{\sim}{\hookrightarrow} S(\{a, b, c\}) \simeq S_3$$



例如 $\rho^{-1}(ab)$

$$\begin{aligned} \rho^{-1}(ab) : K &\xrightarrow{\sim} K \\ \sqrt[3]{2} &\longmapsto \sqrt[3]{2}\omega \\ \sqrt[3]{2}\omega &\longmapsto \sqrt[3]{2} \\ \omega &\longmapsto \omega^2 \end{aligned}$$

$< (ab) >$ 对应的不动子域为

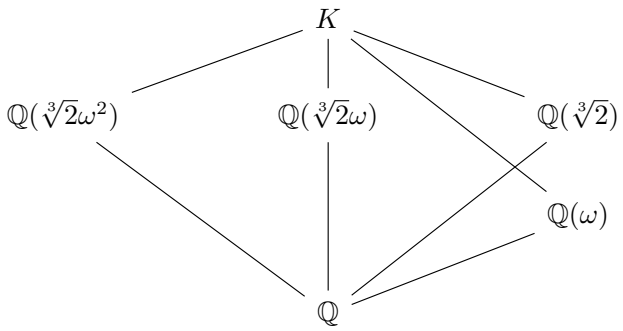
$$K^{<(ab)>} = \{v \in K, \rho^{-1}(ab)(v) = v\}$$

注意到 $\rho^{-1}(ab)(\sqrt[3]{2}\omega^2)=\sqrt[3]{2}\omega^2 \Longrightarrow \sqrt[3]{2}\omega^2 \in K^{<(ab)>}$，则 $\mathbb{Q}(\sqrt[3]{2}\omega^2)\subseteq K^{<(ab)>}$，实际上这是等号！

对于 $\rho^{-1}(abc)$

$$\begin{aligned}\rho^{-1}(abc): K &\longrightarrow K\\ \sqrt[2]{3} &\longmapsto \sqrt[2]{3}\omega\\ \sqrt[2]{3}\omega &\longmapsto \sqrt[2]{3}\omega^2\\ \sqrt[2]{3}\omega^2 &\longmapsto \sqrt[2]{3}\end{aligned}$$

$\Longrightarrow \rho^{-1}(abc)(\omega)=\omega$，进而 $\mathbb{Q}(\omega)\subseteq K^{<(abc)>}$，实际上这是等号！



Ex $\mathbb{Q}(\sqrt{2},\sqrt{3})=K=(\mathbb{Q},(x^2-2)(x^2-3))$，考虑群作用

$$G\curvearrowright \mathrm{Root}_K\big((x^2-2)(x^2-3)\big)=\{\sqrt{2},-\sqrt{2},\sqrt{3},-\sqrt{3}\}\overset{记为}{=}\{a,b,c,d\}$$

画出类似上面例子中的两个图

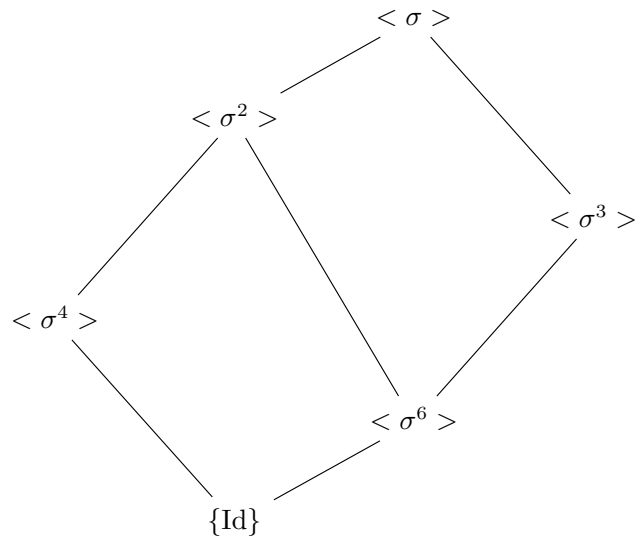
例 5.3 设 K 为有限域，$|K|=p^n$，考虑域扩张 $K/\mathbb{F}_p$，故 $K=(\mathbb{F}_p,x^{p^n}-x)$，考虑 Frobenius 自同构

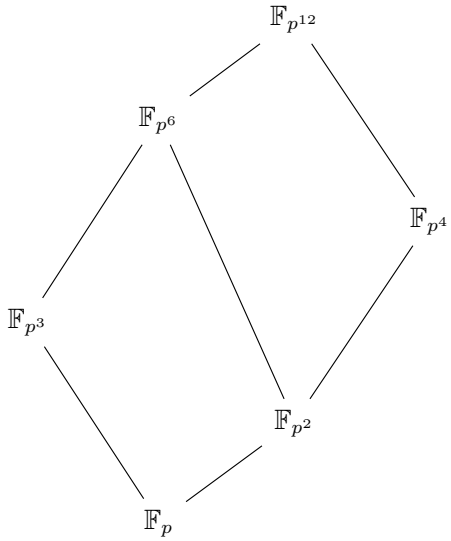
$$\begin{aligned}\sigma: K &\longrightarrow K\\ a &\longmapsto a^p\end{aligned}$$

则 $\mathrm{Gal}(K/\mathbb{F}_p)=\{1,\sigma,\cdots,\sigma^{n-1}\}=<\sigma>$，因此

$$\begin{aligned}\{<\sigma>\text{的子群}\} &\overset{1:1}{\longleftrightarrow} \{K\text{的子域}\}\\ <\sigma^d> &\longmapsto K^{<\sigma^d>}=\{a\in K, a^{p^d}=a\}=\mathrm{Root}_K(x^{p^d}-x)\end{aligned}$$

例如 $n=12$





评价 不是我故意要画那么丑，此处通过高低不同区分子群/中间域的阶数不同

例 5.4 由 Cayley 定理，对任意有限群 $G, \exists n \in \mathbb{N}, \text{s.t. } G \leq S_n$，考虑群作用 $S_n \curvearrowright k(t_1, \cdots, t_n)$，其中 $k(t_1, \cdots, t_n) = \text{Frac}(k[t_1, \cdots, t_n])$ 为 n 元有理函数域，对 $\forall \sigma \in S_n, \sigma(t_i) = t_{\sigma(i)}$，故有 $G \leq S_n \hookrightarrow \text{Aut}(k(t_1, \cdots, t_n))$，即 G 可视为 $\text{Aut}(k(t_1, \cdots, t_n))$ 的子群，所以由定理 5.1.1

$$G \simeq \text{Gal}\left(k(t_1, \cdots, t_n)/k(t_1, \cdots, t_n)^G\right)$$

即任意有限群都可以看作某一 Galois 扩张的 Galois 群

§5.2 偏序集与 Galois 对应

定义 5.2.1（偏序集 partially ordered set）称二元组 $(L, \leq) \overset{\text{记为}}{=} L$（要求 $L \neq \varnothing$）为偏序集，若
(1) 自反性：$a \leq a, \forall a \in L$
(2) 传递性：$a \leq b, b \leq c \Longrightarrow a \leq c$
(3) 对称性：$a \leq b, b \leq a \Longrightarrow a = b$

例 5.5 设 G 是群，则子群关系 $\leq$ 为序关系，此时有偏序集 $(\text{Sub}(G), \leq)$，其中 $\text{Sub}(G) = \{H : H \leq G\}$

例 5.6 考虑域扩张 K/k，则集合的包含关系 $\subseteq$ 为序关系，此时有偏序集 $(\text{Lat}(K/k), \subseteq)$，其中 $\text{Lat}(K/k) = \{K/k\text{的中间域}\}$

定义 5.2.2（最大下界、最小上界）给定偏序集 $(L, \leq)$，定义
(1) $\forall a, b \in L$，称 $a \vee b \in L$ 为 a, b 的最小上界，它满足
  (a) $a \leq (a \vee b), b \leq (a \vee b)$
  (b) 若 $\exists c \in L, \text{s.t. } a \leq c, b \leq c$，则 $(a \vee b) \leq c$
(2) $\forall a, b \in L$，称 $a \wedge b \in L$ 为 a, b 的最大下界，它满足
  (a) $(a \wedge b) \leq a, (a \wedge b) \leq b$
  (b) 若 $\exists c \in L, \text{s.t. } c \leq a, c \leq b$，则 $c \leq (a \wedge b)$

定义 5.2.3（格）称偏序集 $(L,\leq)$ 为格，若 $\forall a,b\in L, a\vee b, a\wedge b$ 存在

例 5.7 G 的子群格 $\mathrm{Sub}(G)$ 是 G 的子群格：对于 $\forall H,V\leq G$

1. $H\wedge V=H\cap U$
2. $H\vee V=<H\cup V>$，即 $H\cup V$ 的生成子群

评价 若 $H\leq G, N\lhd G$，则 $H\vee N=HN=NH$

例 5.8 域扩张的中间域格 $\mathrm{Lat}(K/k)$ 是域扩张 K/k 的中间域格：对于 $k\subseteq E,F\subseteq K$

1. $E\wedge F=E\cap F$
2. $E\vee F=$ 包含$E\cup F$的最小子域，即由 $E\cup F$ 生成的域

例 5.9（反格）设 $(L,\leq)$ 为格，则 $(L^{\mathrm{op}},\leq^{\mathrm{op}})$ 也是格，其中作为集合有 $L^{\mathrm{op}}=L$，$\leq^{\mathrm{op}}$ 定义为

$$a\leq^{\mathrm{op}} b \iff b\leq a$$

且 $a\wedge^{\mathrm{op}} b=a\vee b, a\vee^{\mathrm{op}} b=a\wedge b$

例 5.10 对 $\forall n\geq 1$，定义 $L_n=\{d:1\leq d\leq n, d\mid n\}$，其中序关系定义为 $a\preceq b\iff a\mid b$，则 $(L_n,\preceq)$ 为格，最小上界为 lcm，最大下界为 gcd

定义 5.2.4（偏序集的同态、同构）称 $f:(L_1,\leq)\longrightarrow(L_2,\preceq)$，若
(1) $f:L_1\to L_2$ 是映射
(2) f 保序：若 $x\leq y$ in L_1，则 $f(x)\preceq f(y)$ in L_2
若 f 为双射，且 f^{-1} 也是偏序集的同态，则称 f 是偏序集的同构

引理 5.2.1 设 L,L' 均为格，$f:L\xrightarrow{\sim}L'$ 为偏序集同构，则 f 保最小上界和最大下界，即

$$f(a\vee b)=f(a)\vee f(b),\quad f(a\wedge b)=f(a)\wedge f(b),\quad \forall a,b\in L$$

Ex 证明上述引理

例 5.11 f^{-1} 不保序，不保最小上界/最大下界：取 $n=12$，考虑偏序集的同态

$$f:(\{1,2,3,4,6,12\},\leq)\to(L_{12},\preceq)$$

它是双射，但是在 $\{1,2,3,4,6,12\}$ 中，$4\vee 6=6$，而在 L_{12} 中，$4\vee 6=12$

例 5.12 考虑 n 阶循环群 $C_n=<g:g^n=1>$，则有格同构

$$\begin{array}{ccc}\mathrm{Sub}(C_n) & \xleftrightarrow{1:1} & (L_n,\preceq)\\ <g^{\frac{n}{d}}> & \longmapsto & d\end{array}$$

回忆 G-集 (X,ψ) 的定义：设有群作用 $G\curvearrowright X$ 定义为映射 $\psi: G\times X\to X$，则称 (X,ψ) 为 G-集，类似地，我们如下定义 G-偏序集

定义 5.2.5（G-偏序集）若存在群作用 $G\curvearrowright L$，我们可以定义 G-偏序集（G-poset）为：
(1) $(L,\preceq)$ 是偏序集
(2) 有群作用 $G\curvearrowright L$，对应的群同态为 $\rho: G\longrightarrow \mathrm{Aut}(L,\preceq)$
(3) 相容性：对 $\forall g\in G, a\preceq b \iff g.a\preceq g.b$

例 5.13 $G\curvearrowright \mathrm{Sub}(G)$

$$g.H = gHg^{-1}$$

因为 $H\le U\Longrightarrow gHg^{-1}\le gUg^{-1}$，故满足相容性

例 5.14 $\mathrm{Gal}(K/k)=G\curvearrowright \mathrm{Lat}(K/k)$

$$\sigma.E=\sigma(E)=\{\sigma(v): v\in E\}$$

设 $E_1\subseteq E_2$，由定义显然有 $\sigma(E_1)\subseteq\sigma(E_2)$，故满足相容性

定理 5.2.1（Galois 理论的基本定理）设 K/k 是有限维 Galois 扩张，$G=\mathrm{Gal}(K/k)$，则有格同构（G-偏序集同构）

$$\begin{aligned}\mathrm{Sub}(G)&\xrightarrow{\sim}\mathrm{Lat}(K/k)^{\mathrm{op}}\\ H&\longmapsto K^H\\ \mathrm{Gal}(K/E)&\longmapsfrom E\end{aligned}$$

且 ϕ 满足
(1) ϕ 保最小上界 $\vee$ 和最大下界 $\wedge$
(2) ϕ 保 G-作用，即
- $K^{\sigma H\sigma^{-1}}=\sigma(K^H)$
- $\mathrm{Gal}(K/\sigma(E))=\sigma(\mathrm{Gal}(K/E))\sigma^{-1}$

证明 只证明 (2)，因为

$$\begin{aligned}x\in K^{\sigma H\sigma^{-1}}&\iff \forall\tau\in H,\sigma\tau\sigma^{-1}(x)=x\\ &\iff \forall\tau\in H,\tau(\sigma^{-1}(x))=\sigma^{-1}(x)\\ &\iff \sigma^{-1}(x)\in K^H\\ &\iff x\in\sigma(K^H)\end{aligned}$$

所以 $K^{\sigma H\sigma^{-1}}=\sigma(K^H)$，又因为

$$\begin{aligned}\mathrm{Gal}(K/\sigma(E))&=\{\delta\in\mathrm{Aut}(E):\delta\circ\sigma(e)=\sigma(e),\forall e\in E\}\\ &=\{\delta\in\mathrm{Aut}(K):(\sigma^{-1}\circ\delta\circ\sigma)|_E=\mathrm{Id}_E\}\\ &=\sigma\mathrm{Gal}(K/E)\sigma^{-1}\end{aligned}$$

□

推论 5.2.1 设 K/k 为有限维 Galois 扩张，$G=\mathrm{Gal}(K/k)$，则

(1) 设 $k\subseteq E\subseteq K$，则 $K^{\mathrm{Gal}(K/E)}=E$，且 $[E:k]=[G:\mathrm{Gal}(K/E)]$

(2) 设 $H\leq G$，则 $\mathrm{Gal}(K/K^H)=H$，且 $[G:H]=[K^H:k]$

证明 考虑定理5.2.1，有恒等映射 $H\mapsto K^H\mapsto \mathrm{Gal}(K/K^H), E\mapsto \mathrm{Gal}(K/E)\mapsto K^{\mathrm{Gal}(K/E)}$，所以

$$K^{\mathrm{Gal}(K/E)}=E,\quad \mathrm{Gal}(K/K^H)=H$$

只证明 (2) 中等式，(1) 中等式类似，由定理5.1.1、维数公式和 Lagrange 定理

$$\begin{cases}|G|=[G:H]\cdot|H|\\ [K:k]=[K^H:k]\cdot[K:K^H]\\ |H|=[K:K^H],|G|=[K:k]\end{cases}\Longrightarrow [G:H]=[K^H:k]$$

□

推论 5.2.2 设 K/k 为有限维 Galois 扩张，$G=\mathrm{Gal}(K/k)$，则

(1) 设 $H,U\leq G$，则

$$\begin{cases}K^H\cap K^U\overset{\text{平凡}}{=}K^{H\vee U}\\ K^H\wedge K^U\overset{\text{不平凡}}{=}K^{H\cap U}\end{cases}$$

(2) 设 $k\subseteq F,E\subseteq K$，则

$$\begin{cases}\mathrm{Gal}(K/(F\vee E))=\mathrm{Gal}(K/F)\cap\mathrm{Gal}(K/E)\\ \mathrm{Gal}(K/(F\cap E))=\mathrm{Gal}(K/F)\vee\mathrm{Gal}(K/E)\end{cases}$$

推论 5.2.3 $\mathrm{Sub}(G)$ 和 $\mathrm{Lat}(K/k)^{\mathrm{op}}$ 在 G-作用下的不动点集为

$$\begin{cases}\mathrm{Sub}(G)^G=\{H\leq G:\sigma H\sigma^{-1}=H,\forall\sigma\in G\}=\{H:H\lhd G\}\\ (\mathrm{Lat}(K/k)^{\mathrm{op}})^G=\{E:E\text{是}K/k\text{的中间域},\sigma(E)=E,\forall\sigma\in G\}\\ \qquad\qquad=\{E:E/k\text{为有限维Galois扩张}\}\end{cases}$$

其中第二行的第二个等号是因为命题 5.1.1

推论 5.2.4 有不动子群同构

$$\mathrm{Sub}(G)^G\xrightarrow{\sim}(\mathrm{Lat}(K/k)^{\mathrm{op}})^G$$

考虑域扩张塔 $k\subseteq E\subseteq K$，则 $\mathrm{Gal}(K/E)\lhd G\iff E/k$ 是有限维 Galois 扩张，此时称 E 是 K 的正规子域，且有群同构

$$G/\mathrm{Gal}(K/E)\simeq\mathrm{Gal}(E/k)$$

证明 考虑满同态（满射由延拓定理知）

$$\begin{aligned}\theta : G &\longrightarrow \mathrm{Gal}(E/k)\\ \sigma &\longmapsto \sigma|_E\end{aligned}$$

因为 $\mathrm{Ker}\theta = \mathrm{Gal}(K/E)$，由群同态基本定理即证 □

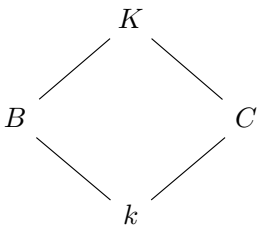
评价 对于推论5.2.4中的同构，考虑 $H \leq G$ 的稳定化子 $G_H = \{\sigma \in G : \sigma H \sigma^{-1} = H\}$，对应地，$K_H$ 的稳定化子为 $G_{(K^H)} = \{\sigma \in G : \sigma(K^H) = K^H\}$，它们实际上有如下关系

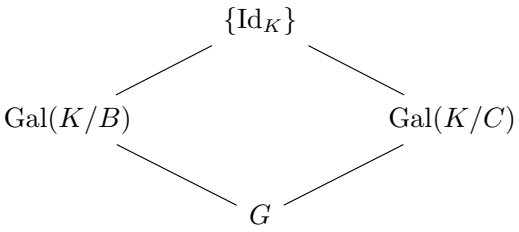
Ex 证明 $\mathrm{Gal}(K^H/k) = G_H/H$

评价 这个练习不是那么平凡，需要一些慧眼

> **命题 5.2.1** 设 $f(x), g(x) \in k[x]$ 可分，$K = (k, f(x)g(x)), B = (k, f(x)), C = (k, g(x))$，若 $B \cap C = k$，则
>
> $$\mathrm{Gal}(K/k) \simeq \mathrm{Gal}(B/k) \times \mathrm{Gal}(C/k)$$

证明 记 $G = \mathrm{Gal}(K/k)$





注意到 $B \cap C = k, B \vee C = K$，由定理5.2.1知

$$\begin{cases}\mathrm{Gal}(K/B) \vee \mathrm{Gal}(K/C) = G\\ \mathrm{Gal}(K/B) \cap \mathrm{Gal}(K/C) = \{\mathrm{Id}\}\end{cases}$$

由 f, g 可分知，$B/k, C/k$ 是 Galois 扩张，所以 $\mathrm{Gal}(K/B) \lhd G, \mathrm{Gal}(K/C) \lhd G$，则 $G = \mathrm{Gal}(K/B) \vee \mathrm{Gal}(K/B) = \mathrm{Gal}(K/B)\mathrm{Gal}(K/C)$，由下面的练习知

$$G = \mathrm{Gal}(K/B)\mathrm{Gal}(K/C) \simeq \frac{\mathrm{Gal}(K/k)}{\mathrm{Gal}(K/B)} \times \frac{\mathrm{Gal}(K/k)}{\mathrm{Gal}(K/C)} \overset{\text{Cor } 5.2.4}{\simeq} \mathrm{Gal}(B/k) \times \mathrm{Gal}(C/k)$$

Ex 设 $N_1 \lhd G, N_2 \lhd G$，且 $N_1 N_2 = G, N_1 \cap N_2 = \{1_G\}$，则 $G \simeq (G/N_1) \times (G/N_2)$

例 5.15 设 $K = (\mathbb{Q}, (x^2-2)(x^2-3)), B = \mathbb{Q}(\sqrt{2}), C = \mathbb{Q}(\sqrt{3})$，则由上面的命题知

$$\mathrm{Gal}(K/\mathbb{Q}) \simeq \mu_2 \times \mu_2$$

定理 5.2.2（Steinitz, 1910）设 K/k 是有限维域扩张，则 K/k 是单扩张 $\iff$ K/k 只有有限个中间域

证明 $(\Longrightarrow)$：设 $K=k(\alpha)$，α 在 k 上的最小多项式为 $f(x)$，考虑域扩张塔

$$k\subseteq E\subseteq K$$

设 α 在 E 上的最小多项式为 $g(x)=x^m+c_1x^{m-1}+\cdots+c_m, c_i\in E$，则 $E\supseteq B=k(c_1,\cdots,c_m)$

***Claim*:** $E=B$

Proof Of Claim：只需证明 $E\subseteq B$，因为 $\dim_E K=m=\dim_B K$，由维数公式知 $\dim_B E=1$，故 $E=B$

又因为 $g(x)\mid f(x)$ in $k[x]$，且 $f(x)$ 只有有限多个因子，故只有有限多个中间域

$(\Longleftarrow)$：若 $|k|<+\infty$，则 $k\simeq\mathbb{F}_{p^n}$ 为单扩张，下面设 $|k|=+\infty$，设 $K=k(\alpha_1,\cdots,\alpha_t)$，考虑域扩张塔

$$k\subseteq k(\alpha_1,\alpha_2)\subseteq K$$

对 $\forall\lambda\in k$，设 $E_\lambda=k(\alpha_1+\lambda\alpha_2)$，由只有有限多个中间域知 $\exists\lambda_1\neq\lambda_2,\text{s.t. }E_{\lambda_1}=E_{\lambda_2}$，因为

$$\begin{cases}\alpha_1+\lambda_1\alpha_2\in E_{\lambda_1}\\ \alpha_1+\lambda_2\alpha_2\in E_{\lambda_2}\end{cases}\Longrightarrow\alpha_1,\alpha_2\in E_{\lambda_1}=E_{\lambda_2}$$

因此 $k(\alpha_1,\alpha_2)=k(\alpha_1+\lambda_1\alpha_2)=k(\alpha_1+\lambda_2\alpha_2)$ 是单扩张，由数学归纳法可知 K/k 是单扩张 □

评价 若 K/k 是有限维单扩张，对于 $\forall k\subseteq E\subseteq K$，因为 E/k 只有有限多个中间域，所以 E/k 是单扩张

定理 5.2.3（本原元定理 ,Galois）设 K/k 是有限维可分扩张（$\forall\alpha\in K$，α 在 k 上的最小多项式可分），则 K/k 是单扩张

证明 设 $K=k(\alpha_1,\cdots,\alpha_t)$，$\alpha_i$ 在 k 上的最小多项式为 $g_i(x)$，取 $E=(K,g_1(x)\cdots g_t(x))$，则 $k\subseteq K\subseteq E$，且 E/k 也是分裂域，由可分知 E/k 是 Galois 扩张，故 E/k 只有有限多个中间域，由上面的注记知 K/k 也只有有限多个中间域，故 K/k 是单扩张 □

评价 Galois 扩张是可分扩张，因此是单扩张

例 5.16 $k=\mathbb{F}_p(t_1,t_2),K=(k,(x^p-t_1)(x^p-t_2))$，则在 K 上有（作业做过）

$$(x^p-t_1)(x^p-t_2)=(x-a)^p(x-b)^p,\quad\exists a,b\in K,a^p=t_1,b^p=t_2$$

则 $K=k(a,b)$，由 Eisenstein 判别法知 x^p-t_1,x^p-t_2 不可约，由下面练习可知定理5.2.3中的可分条件是必要的

Ex 证明

1. $\dim_k K=p^2$
2. $\mathrm{Gal}(K/k)=\{\mathrm{Id}\}$

3. $\forall \lambda \in k$，定义 $E_\lambda = k(a+\lambda b)$，则
   - $\dim_k E_\lambda = p$
   - $E_\lambda \neq E_\mu, \forall \lambda \neq \mu$

接下来利用 Galois 理论证明代数学基本定理（Fundamental Theorem of Algebra），首先需要引理如下

引理 5.2.2
(1) 若 $\mathbb{R} \subsetneq K$，则 $\dim_{\mathbb{R}} K$ 为偶数
(2) 若 $\mathbb{C} \subseteq K$，则 $\dim_{\mathbb{C}} K \neq 2$

证明
(1) 对 $\forall \alpha \in K \backslash \mathbb{R}$，设 α 的最小多项式为 $f(x)$，则 $\deg f(x) \mid \dim_{\mathbb{R}} K$，假设 $\dim_{\mathbb{R}} K$ 为奇数，则 $\deg f(x)$ 也为奇数，奇数次多项式一定有实根，这与 f 在 $\mathbb{R}$ 上不可约矛盾！
(2) 假设 $\dim_{\mathbb{C}} K = 2$，则 $\exists \alpha \in K \backslash \mathbb{C}, \text{s.t. } K = \mathbb{C}(\alpha)$，设 α 在 $\mathbb{C}$ 上的最小多项式为 x^2+ax+b，由求根公式知 $\alpha = \frac{-a \pm \sqrt{a^2-4b}}{2} \in \mathbb{C}$，矛盾！ □

定理 5.2.4（代数基本定理） $\mathbb{C}$ 是代数封闭域，i.e $\forall f(x) \in \mathbb{C}[x]$ 有复根

证明 设 $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{C}[x]$ 不可约，考虑 $\overline{f}(x) = \sum_{i=0}^{n} \overline{a}_i x^i$，则

$$f(x)\overline{f}(x) = \sum_{k=0}^{2n} c_k x^k, \quad c_k = \sum_{i+j=k} a_i \overline{a}_j$$

易见 $c_k = \overline{c}_k$，即 $f(x)\overline{f}(x) \in \mathbb{R}[x]$，因为 $f(x)$ 有复根 $\iff$ $f(x)\overline{f}(x)$ 有复根，所以我们只需证明 $\forall p(x) \in \mathbb{R}[x]$ 有复根

***Claim*:** 设 $p(x) \in \mathbb{R}[x]$ 不可约，$K/\mathbb{R}$ 为 $(x^2+1)p(x)$ 的分裂域，则 $K/\mathbb{R}$ 是 *Galois* 扩张
Proof Of Claim : 由 $\text{Char}(\mathbb{R}) = 0$ 知，$(x^2+1)p(x)$ 可分，故 $K/\mathbb{R}$ 为有限维 *Galois* 扩张
***Claim*:** 设 $G = \text{Gal}(K/\mathbb{R})$，则 $|G| = 2^r$
Proof Of Claim : 否则，$|G| = 2^r m, m$ 是奇数，由 *Sylow* 定理知 G 有 *Sylow-2* 子群 P，则 $[G:P] = m$，考虑域扩张塔

$$\mathbb{R} \subseteq K^P \subseteq K$$

因为 $[K^P : \mathbb{R}] = m$，由引理5.2.2(1) 知 $m = 1$，故 $\dim_{\mathbb{C}} K = \frac{\dim_{\mathbb{R}} K}{\dim_{\mathbb{R}} \mathbb{C}} = 2^{r-1}$，设 $G' = \text{Gal}(K/\mathbb{C})$，则由定理5.1.1知 $|G'| = 2^{r-1}$ 再由下面的练习知，$\exists H \leq G', \text{s.t. } [G':H] = 2$，考虑如下域扩张塔

$$\mathbb{C} \subseteq K^H \subseteq K$$

因为 $\dim_{\mathbb{C}} K^H = [G':H] = 2$，这与引理5.2.2(2) 矛盾！ □

Ex 设 U 是 p-群，则 $\exists V \leq U, \text{s.t. } [U:V] = p$

评价 考虑 $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$，则 $\mathbb{Q}(\sqrt{2})/\mathbb{Q}, \mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ 是 *Galois* 扩张，但是 $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ 不是 *Galois* 扩张

§5.3 根式扩张与 Galois 大定理

定义 5.3.1（根式扩张、根式扩张塔）称 E/k 是根式扩张 (of type m)，若 $E=k(\alpha)$，且 $\alpha^m=a\in k$；称域扩张塔

$$k=E_0\subseteq E_1\subseteq\cdots\subseteq E_n$$

为根式扩张塔，若 $E_i/E_{i-1}, 1\le i\le n$ 为根式扩张

评价 形象的记号：$\alpha=\sqrt[m]{a}$，但是一般不这么写

定义 5.3.2（根式可解）称 $f(x)\in k[x]$ 根式可解，若存在根式扩张塔

$$k\subseteq E_0\subseteq E_1\subseteq\cdots\subseteq E_n$$

使得 $f(x)$ 在 E_n 中分裂，即 $(k,f(x))\subseteq E_n$

例 5.17 设 $f(x)=x^2+bx+c\in\mathbb{C}[x]$，则 $k\overset{\text{def}}{=}\mathbb{Q}(b,c)\subseteq\mathbb{C}$，我们有

$$k=E_0\subseteq E_1=k(\sqrt{b^2-4c})=k(\alpha)$$

取 $\alpha\in\mathbb{C}$, s.t. $\alpha^2=b^2-4c$，则 $k(\alpha)/k$ 是根式扩张

Fact 设 $E=k(\alpha),\alpha^m=a\in k$，则

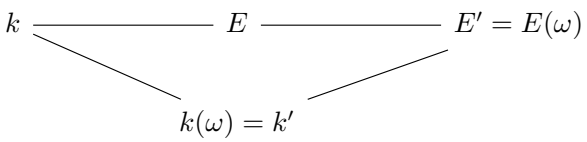
(1) k 恰有 m 次本原单位根 ω，则 $(x^m-a)=\prod_{i=1}^{m}(x-\omega^i\alpha)$ in $E[x]$，进而 $E=(k,x^m-a)$，且由 x^m-a 无重根知，它在 k 上可分，故 E/k 是 Galois 扩张，此时

$$\mathrm{Gal}(E/k)=\{\mathrm{Id},\sigma_1,\cdots,\sigma_{m-1}\},\quad \sigma_i(\alpha)=\omega^i\alpha$$

有群嵌入（因此 $\mathrm{Gal}(E/k)$ 是 *Abel* 群）

$$\begin{aligned}\mathrm{Gal}(E/k)&\hookrightarrow(\mathbb{Z}_m,+)\\ \sigma_i&\longmapsto\bar{i}\end{aligned}$$

(2) 若 $\mathrm{Char}(k)=0$，考虑 $E'=(E,x^m-1)=E(\omega),\omega$ 为 m 次本原单位根，此时有域扩张塔



因此

- 由 (1) 知 $\mathrm{Gal}(E'/k')\hookrightarrow(\mathbb{Z}_m,+)$，故 $\mathrm{Gal}(E'/k')$ 为 Abel 群
- 因为 k'/k 为分圆域扩张，所以 $\mathrm{Gal}(k'/k)\hookrightarrow U(\mathbb{Z}_m)$，且 $\mathrm{Gal}(k'/k)$ 为 Abel 群

考虑域扩张塔 $k\subseteq k'\subseteq E'$，因为 $k'=k(\omega)=(k,\Phi_m(x))$，所以 k'/k 是 Galois 扩张，故

$$\mathrm{Gal}(E'/k')\lhd\mathrm{Gal}(E'/k),\quad \mathrm{Gal}(E'/k)/\mathrm{Gal}(E'/k')\simeq\mathrm{Gal}(k'/k)$$

可以用如下群的正合列表示

$$1 \longrightarrow \mathrm{Gal}(E'/k') \overset{\lhd}{\hookrightarrow} \mathrm{Gal}(E'/k) \twoheadrightarrow \mathrm{Gal}(K'/k) \longrightarrow 1$$

故有满射 $\mathrm{Gal}(E'/k) \twoheadrightarrow \mathrm{Gal}(E/k)$，且有（我不太懂）

$$\mathrm{Gal}(E/k) \xrightarrow{\sim} N(\mathrm{Gal}(E'/E))/\mathrm{Gal}(E'/E)$$

引理 5.3.1 若 $\mathrm{Char}(k) = 0$，则任意根式扩张塔可以扩张成 Galois 扩张，即 $k = E_0 \subseteq \cdots \subseteq E_n$ 可延长至

$$k = E_0 \subseteq \cdots \subseteq E_n \subseteq \cdots \subseteq E_m$$

满足 E_m/k 是 Galois 扩张

评价 这个引理的作用：可以不妨设根式扩张塔 $k = E_0 \subseteq \cdots \subseteq E_n$ 中，E_n/k 是 Galois 扩张

证明 由本原元定理5.2.3，可设 $E_n = k(\beta)$，β 在 k 上的最小多项式为 $f(x)$，取 $K = (E_n, f(x))$，则有域扩张塔

$$k \subseteq E_n \subseteq K$$

由根式扩张知 f 在 E_n 上可分，故 K/k 是 Galois 扩张，设 $\mathrm{Gal}(K/k) = \{\sigma_0 = \mathrm{Id}, \sigma_1, \cdots, \sigma_p\}$

***Claim*:** $E_n \subseteq E_n \vee \sigma_1(E_n)$ 可表示为根式扩张塔

Proof Of Claim : 考虑如下域扩张塔

$$E_n \subseteq E_n \vee \sigma_1(E_1) \subseteq E_n \vee \sigma_1(E_2) \subseteq \cdots \subseteq E_n \vee \sigma_1(E_n)$$

因为 E_1/k 为根式扩张，所以 $E_n \vee \sigma_1(E_1)/E_n$ 为根式扩张；因为 E_2/E_1 是根式扩张，所以 $(E_n \vee \sigma_1(E_2))/(E_n \vee \sigma_1(E_1))$ 是根式扩张；依此类推知 $E_n \subseteq E_n \vee \sigma_1(E_n)$ 可表示为根式扩张塔，对 $\sigma_2, \cdots, \sigma_p$ 进行类似操作，故有根式扩张塔

$$k \subseteq E_n \subseteq E_n \vee \sigma_1(E_n) \subseteq E_n \vee \sigma_1(E_n) \vee \sigma_2(E_n) \subseteq \cdots \subseteq E_n \vee \sigma_1(E_n) \vee \cdots \vee \sigma_p(E_n) = K$$

（需要完成下面的练习），进而 $K/k = (E_n, f(x))/k$ 为 Galois 扩张 □

Ex 验证 $E_n \vee \sigma_1(E_n) \vee \cdots \vee \sigma_p(E_n) = K$

Fact（此部分为了证明 Galois 大定理准备的，可以先跳转到可解群部分）

(1) 设有根式扩张塔 $k = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_n$，不妨设 E_n/k 是 Galois 扩张，假设 k 有充分多[1]的单位根，根据上一个 Fact，每个 E_i/E_{i-1} 都是 Galois 扩张，每个 $\mathrm{Gal}(E_i/E_{i-1})$ 都是 Abel 群，对应有 Galois 群的下降列（由 Galois 扩张知前一个群是后一个群的正规子群）

$$\mathrm{Gal}(E_n/E_0) \trianglerighteq \mathrm{Gal}(E_n/E_1) \trianglerighteq \mathrm{Gal}(E_n/E_2) \trianglerighteq \cdots \trianglerighteq \{\mathrm{Id}\}$$

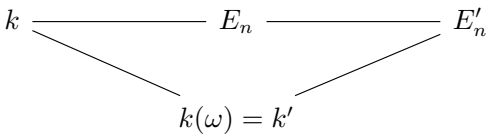
[1] 充分多表示 k 中包含根式扩张塔中所有 type 的单位根

由推论5.2.4，相邻的群做商得（称为因子）

$$\mathrm{Gal}(E_n/E_0)/\mathrm{Gal}(E_n/E_1)\simeq\mathrm{Gal}(E_1/E_0),\quad \mathrm{Gal}(E_n/E_1)/\mathrm{Gal}(E_n/E_2)\simeq\mathrm{Gal}(E_2/E_1),\quad\cdots$$

所以 $\mathrm{Gal}(E_1/E_0),\mathrm{Gal}(E_2/E_1),\cdots,\mathrm{Gal}(E_n/E_{n-1})$ 均为 Abel 群

(2) 一般地，设 $\mathrm{Char}(k)=0$，假设 k 没有足够的单位根，设有根式扩张塔 $k=E_0\subseteq E_1\subseteq\cdots\subseteq E_n$，不妨设 E_n/k 是 Galois 扩张，设每个根式扩张 E_i/E_{i-1} 的 type 为 m_i，记 $M=\mathrm{lcm}(m_1,\cdots,m_n)$，考虑 $E_n'=(E_n,x^M-1)$，记 ω 为 M 次本原单位根，考虑域扩张塔



故有群正合列

$$1\longrightarrow\mathrm{Gal}(E_n'/k')\xrightarrow{\trianglelefteq}\mathrm{Gal}(E_n'/k)\twoheadrightarrow\mathrm{Gal}(k'/k)\longrightarrow 1$$
$$\mathrm{Gal}(E_n/k)$$

回忆：若 $f(x)\in k[x],\mathrm{Gal}_k(f)=\mathrm{Gal}((k,f(x))/k)$，若 f 根式可解，即存在根式扩张塔

$$k=E_0\subseteq\cdots\subseteq E_n$$

（可不妨设 E_n/k 是 Galois 扩张）使得 $f(x)$ 在 E_n 上分裂，即 $L\overset{\mathrm{def}}{=}(k,f(x))\subseteq E_n$，此时有满射

$$\mathrm{Gal}_k(f)=\mathrm{Gal}(L/k)\twoheadleftarrow\mathrm{Gal}(E_n/k)$$

定义 5.3.3（可解群） 有限群 G 称为可解群 (Solvable)，若存在子群降列

$$G=G_0\trianglerighteq G_1\trianglerighteq G_2\trianglerighteq\cdots\trianglerighteq G_n=\{\mathrm{Id}\}$$

满足 $G_{i+1}\trianglelefteq G_i$，因子 G_i/G_{i+1} 为 Abel 群

例 5.18

$n=1$ 时，$G=G_0\trianglerighteq G_1=\{1_G\}$，因子 $G/\{1_G\}\simeq G$ 为 Abel 群，即 Abel 群可解

例 5.19 $n=2$ 时，$G=G_0\trianglerighteq G_1\trianglerighteq G_2=\{1_G\}$，因子 $G/G_1,G_1/G_2\simeq G_1$ 为 Abel 群，故有群正合列

$$1\longrightarrow G_1\xrightarrow{\trianglelefteq}G\twoheadrightarrow G/G_1\longrightarrow 1$$
$$\text{Abel}\qquad\qquad\text{Abel}$$

例如 S_3 可解：$S_3\trianglerighteq A_3\trianglerighteq\{\mathrm{Id}\}$，即有 $1\to A_3\overset{\trianglelefteq}{\hookrightarrow}S_3\twoheadrightarrow C_2\to 1$，其中 $S_3/A_3\simeq C_2$，C_2 为二阶循环群

例 5.20 $n=3$ 时，$G=G_0\trianglerighteq G_1\trianglerighteq G_2\trianglerighteq G_3=\{1_G\}$，因子 $G/G_1,G_1/G_2,G_2/G_3\simeq G_2$ 为 *Abel* 群，可以表示为两个群正合列

$$\begin{array}{ccccccccc} & & \text{Abel} & & & & \text{Abel} & & \\ & & \vdots & & & & \vdots & & \\ 1 & \longrightarrow & G_2 & \overset{\trianglelefteq}{\hookrightarrow} & G_1 & \twoheadrightarrow & G_1/G_2 & \longrightarrow & 1 \end{array}$$

$$\begin{array}{ccccccccc} & & \vdots & & & & \vdots & & \\ & & \text{Abel} & & & & \text{Abel} & & \\ 1 & \longrightarrow & G_1 & \overset{\trianglelefteq}{\hookrightarrow} & G & \twoheadrightarrow & G/G_1 & \longrightarrow & 1 \end{array}$$

例如 S_4 可解：$S_4 \trianglerighteq A_4 \trianglerighteq K_4 \trianglerighteq \{\mathrm{Id}\}$，即有

$$1 \longrightarrow K_4 \overset{\trianglelefteq}{\hookrightarrow} A_4 \twoheadrightarrow C_3 \longrightarrow 1$$

$$1 \longrightarrow A_4 \overset{\trianglelefteq}{\hookrightarrow} S_4 \twoheadrightarrow C_2 \longrightarrow 1$$

其中 $A_4/K_4 \simeq C_3, S_4/A_4 \simeq C_2$

例 5.21 根据定义，非 Abel 单群不可解！因此 $A_n, n \geq 5$ 不可解，因为 $A_n \leq S_n$，由下面的命题知 $S_n, n \geq 5$ 不可解

命题 5.3.1 设 G 可解，则
(1) 若 $H \leq G$，则 H 可解
(2) 若 $N \trianglelefteq G$，则 G/N 可解

Ex 证明上述事实

Hint : 由 G 可解可设 $G \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_n = \{1_G\}$，考虑

$$\begin{cases} H \trianglerighteq (H \cap G_1) \trianglerighteq (H \cap G_2) \trianglerighteq \cdots \trianglerighteq H \cap G_n = \{1_G\} \\ G/N \trianglerighteq (G_1N)/N \trianglerighteq (G_2N)/N \trianglerighteq \cdots \trianglerighteq (G_nN)/N = \{1_{G/N}\} \end{cases}$$

命题 5.3.2 若 $N \trianglelefteq G$，若 $N, G/N$ 可解，则 G 可解

证明 由 $N, G/N$ 可解可设

$$\begin{cases} N \trianglerighteq N_1 \trianglerighteq N_2 \trianglerighteq \cdots \trianglerighteq N_n = \{1_G\} \\ G/N \trianglerighteq G_1/N \trianglerighteq G_2/N \trianglerighteq \cdots \trianglerighteq N/N = \{1_{G/N}\} \end{cases}$$

由对应定理知有子群降列 $G \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq N$，将它与 N 的子群降列相接得

$$G \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq N \trianglerighteq N_1 \trianglerighteq N_2 \trianglerighteq \cdots \trianglerighteq N_n = \{1_G\}$$

故 G 可解 □

例 5.22 设 G 是 p-群，则 G 可解

证明 设 $|G|=p^n$，对 n 归纳，$n=1$ 时 $|G|=p$，G 为循环群，故为 Abel 群，可解，假设 $n<k$ 时命题均成立，下面证明 $n=k$ 时，因为 p-群 G 有非平凡中心 $Z(G)$

Case 1. 若 $Z(G)=G$，则 G 是 Abel 群，故 G 可解

Case 2. 若 $Z(G)\neq G$，则由 Lagrange 定理知 $|Z(G)|=p^s, s<n, |G/Z(G)|=p^t, t<n$，由归纳假设知 $Z(G), G/Z(G)$ 均可解，又因为 $Z(G)\lhd G$，由命题5.3.2，G 可解 □

引理 5.3.2 设 K/k 是有限维 Galois 扩张，$\mathrm{Gal}(K/k)=<\sigma>, \sigma^p=\mathrm{Id}_K, p$ 素数，若 k 有 p 次本原单位根，则 K/k 是根式扩张 of type p

证明 将 $\sigma: K\to K$ 视为 k-线性同构，因为 $\sigma^p=\mathrm{Id}_K$，且 $\dim_k K=p$，故 x^p-1 为 σ 的特征多项式

因为 p 次本原单位根满足 $\omega^p=1$，所以 ω 为 σ 的特征值，设 $\beta\in K$ 是 ω 所对应的特征向量，则 $\sigma(\beta)=\omega\beta\neq\beta$，则 $\sigma(\beta^p)=(\omega\beta)^p=\beta^p\Longrightarrow\beta^p\in K^{<\sigma>}=k$，考虑域扩张塔

$$k\subsetneqq k(\beta)\subseteq K$$

由维数公式知 $[K:k(\beta)]\cdot[k(\beta):k]=[K:k]=p$，因为 $\beta\notin k$，所以 $[k(\beta):k]>1$，故只能等于 p，进而 $[K:k(\beta)]=1$，$K=k(\beta)$，即 K/k 是根式扩张 of type p □

定理 5.3.1（Galois 大定理）设 $\mathrm{Char}(k)=0, f(x)\in k[x]$，则

$$f(x)\text{根式可解}\iff \mathrm{Gal}_k(f)\text{为可解群}$$

证明 $(\Longrightarrow)$：由根式可解的定义知存在根式扩张塔 $k=E_0\subseteq\cdots\subseteq E_n$，使得 $L=(k,f(x))\subseteq E_n$，由引理5.3.1，可不妨设 E_n/k 是 Galois 扩张，由先前的 Fact(2)知 $\mathrm{Gal}(E_n'/k'), \mathrm{Gal}(k'/k)$ 均为 Abel 群，故它们可解，又因为 $\mathrm{Gal}(k'/k)\simeq\mathrm{Gal}(E_n'/k)/\mathrm{Gal}(E_n'/k')$，由命题5.3.2知 $\mathrm{Gal}(E_n'/k)$ 可解，由 $L\subseteq E_n\subseteq E_n'$ 知，有满射 $\mathrm{Gal}(E_n'/k)\twoheadrightarrow\mathrm{Gal}(E_n/k)\twoheadrightarrow\mathrm{Gal}(L/k)=\mathrm{Gal}_k(f)$，所以由命题5.3.1(1) 知 $\mathrm{Gal}_k(f)$ 可解

$(\Longleftarrow)$：设 $K=(k,f(x)), G=\mathrm{Gal}_k(f)=\mathrm{Gal}(K/k)$ 可解

Case 1. k 有 $|G|$ 次本原单位根，由下面的练习知，$\exists H\lhd G, G/H\simeq C_p, p$ 素数，考虑域扩张塔

$$k\subseteq K^H\subseteq K$$

我们有如下观察

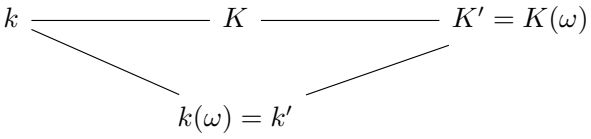
(1) 因为 $\mathrm{Gal}(K/K^H)=H\lhd G$，由推论5.2.4知 K^H/k 是 Galois 扩张

(2) $\mathrm{Gal}(K^H/k)\simeq\mathrm{Gal}(K/k)/\mathrm{Gal}(K/K^H)=G/H\simeq C_p$

由引理5.3.2知，K^H/k 是根式扩张 of type p，因为 $\mathrm{Gal}(K/K^H)=H$ 可解 $(H\lhd G)$

对 H 继续重复上述和 G 一样的操作，可以得到子群降列 $G\rhd H\rhd U\rhd\cdots$ 可解，故有根式扩张塔 $k\subseteq\cdots\subseteq K^U\subseteq K^H\subseteq K$，即 $f(x)$ 根式可解

Case 2. 一般地，考虑 $k\subseteq K\subseteq K'=(K,x^{|G|}-1)=K(\omega)$，其中 ω 是 $|G|$ 次本原单位根



Claim: 有嵌入单同态 $\mathrm{Gal}(K'/k') \hookrightarrow G = \mathrm{Gal}(K/k)$

Proof Of Claim : 考虑映射

$$\begin{aligned} \phi : \mathrm{Gal}(K'/k') &\longrightarrow G = \mathrm{Gal}(K/k) \\ \sigma &\longmapsto \sigma|_K \end{aligned}$$

因为 $K \vee k' = K'$，所以

$$\begin{aligned} \sigma \in \mathrm{Ker}(\phi) &\iff \sigma|_K = \mathrm{Id}_K, \sigma|_{k'} = \mathrm{Id}_{k'} \\ &\overset{K\vee k' = K'}{\iff} \sigma|_{K'} = \mathrm{Id}_{K'} \\ &\iff \sigma = \mathrm{Id}_{K'} \end{aligned}$$

所以 $\mathrm{Ker}(\phi) = \{\mathrm{Id}_{K'}\}$，即 ϕ 为单射

由 Case 1 知，$k(\omega) \subseteq K' = K(\omega)$ 可表示为根式扩张塔，故 $k \subseteq k(\omega) \subseteq K' = (k(\omega), f(x))$ 为根式扩张塔，则 $f(x)$ 根式可解 □

Ex 若 G 可解，则 $\exists H \lhd G, \text{s.t. } G/H \simeq C_p, p$ 是素数

例 5.23 设 $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x], G = \mathrm{Gal}_{\mathbb{Q}}(f) = \mathrm{Gal}(E/\mathbb{Q})$，设 $\mathrm{Root}_{\mathbb{C}}(f) = \{z_1, \cdots, z_5\}$，设 $E = \mathbb{Q}(z_1, \cdots, z_5)$，则有如下观察

(1) $f(x)$ 不可约 $\Longrightarrow z_i, 1 \le i \le 5$ 在 $\mathbb{Q}$ 上的最小多项式为 $f(x)$

(2) f 有三个实根，设为 z_3, z_4, z_5，两个虚根 z_1, z_2 共轭

(3) $|\mathrm{Gal}_{\mathbb{Q}}(f)| = \dim_{\mathbb{Q}} E$

考虑群作用 $G \curvearrowright \mathrm{Root}_{\mathbb{C}}(f) \overset{\text{def}}{=} X$，对应有群同态

$$\begin{aligned} G &\overset{\rho}{\hookrightarrow} S(X) \simeq S_5 \\ \sigma &\longmapsto \sigma|_X \end{aligned}$$

因此可视 $\rho(G)$ 为 S_5 的子群，考虑域扩张塔 $\mathbb{Q} \subseteq \mathbb{Q}(z_1) \subseteq E$，则 $[\mathbb{Q}(z_1) : \mathbb{Q}] = 5 \mid |G|$，故 $\rho(G)$ 有 5 阶元 $\Longrightarrow \rho(G)$ 有 5-循环

再考虑复共轭 $\tau : E \overset{\sim}{\to} E, z \mapsto \overline{z}$，$\rho(\tau)$ 为对换 $(z_1 z_2)$，在 S_5 中即为 (12)，我们有如下事实

Fact (12) 以及任意 5-循环生成 S_5（将 5 换为任意素数 p 都对）

进而 ρ 是满射，故为双射，即 $G \simeq \rho(G) \simeq S_5$，由 Galois 大定理以及 S_5 不可解知，$f(x)$ 根式不可解

定理 5.3.2 考虑 n 元有理函数域 $F = k(t_1, \cdots, t_n)$，定义一般方程如下

$$f(x) = x^n - t_1 x^{n-1} + t_2 x^{n-2} + \cdots + (-1)^n t_n \in F[x]$$

则 $\boxed{\mathrm{Gal}_F(f) \simeq S_n}$，进而若 $\mathrm{Char}(k) = 0$，则 $\mathrm{Char}(F) = 0, \forall n \ge 5$，即 f 不根式可解

证明 设 $y_1, \cdots, y_n$ 是字母，考虑群作用 $S_n \curvearrowright k[y_1, \cdots, y_n]$

$$\begin{aligned} (S_n, k[y_1, \cdots, y_n]) &\longrightarrow k[y_1, \cdots, y_n] \\ (\sigma, f) &\longmapsto f(y_{\sigma(1)}, \cdots, y_{\sigma(n)}) \end{aligned}$$

我们有如下事实（没来得及证明）

Fact 有群同构

$$\begin{aligned} k[t_1,\cdots,t_n] &\xrightarrow{\sim} k[y_1,\cdots,y_n]^{S_n} \\ t_1 &\longmapsto y_1+\cdots+y_n \\ t_2 &\longmapsto \sum_{i<j} y_iy_j \\ &\cdots\cdots\cdots \\ t_n &\longmapsto y_1\cdots y_n \end{aligned}$$

它诱导分式域同构

$$k(t_1,\cdots,t_n) \xrightarrow{\sim} k(y_1,\cdots,y_n)^{S_n}$$

又因为 $k(y_1,\cdots,y_n)^{S_n} \subseteq k(y_1,\cdots,y_n)$，取 $\{y_1,\cdots,y_n\}$ 为 f 的根集，考虑下图

$$\begin{array}{ccc} k(y_1,\cdots,y_n)^{s_n} & \xrightarrow{\quad\sim\quad} & F \\ \Big\downarrow & & \Big\| \\ k(y_1,\cdots,y_n) & \longleftarrow & F \end{array}$$

则 $k(y_1,\cdots,y_n)/F$ 为 $f(x)$ 的分裂域，故 $\mathrm{Gal}_F(f)=\mathrm{Gal}(k(y_1,\cdots,y_n)/F)$；又因为群作用对应了群同态 $\rho: S_n \hookrightarrow \mathrm{Aut}(k(y_1,\cdots,y_n))$，故可视 S_n 为 $\mathrm{Aut}(k(y_1,\cdots,y_n))$ 的子群，由定理5.1.1知

$$\mathrm{Gal}_F(f)=\mathrm{Gal}\left(\frac{k(y_1,\cdots,y_n)}{k(y_1,\cdots,y_n)^{S_n}}\right)\simeq S_n$$

评价（Lagrange 定理 $|G|=|H|\cdot[G:H]$ 的由来）考虑对称多项式全体

$$k[y_1,\cdots,y_n]^{S_n}=\{g(y_1,\cdots,y_n)|\sigma(g)=g,\forall\sigma\in S_n\}$$

Lagrange 证明了如下事实：$g(y_1,\cdots,y_n)\in k[y_1,\cdots,y_n]$

1. $G_g=\{\sigma\in S_n|\sigma(g)=g\}\leq S_n$
2. $\mathcal{O}_g=\{\sigma(g)|\sigma\in S_n\}\subseteq k[y_1,\cdots,y_n]$

则 $|G_g|\cdot|\mathcal{O}_g|=|S_n|$，后来人们发现可以推广到一般情形

invarient theory 是当时的研究热门

定义 5.3.4（群的合成列）群 G 的合成列是指子群降列

$$G=G_0\geq G_1\geq\cdots\geq G_n=\{1_G\}$$

满足 $G_i\lhd G_{i-1}, G_{i-1}/G_i$ 是单群，即 G 可由“因子” G_{i-1}/G_i 拼起来

例 5.24 $n=1$ 时，$G=G_0\geq G_1=\{1_G\}$，故 $G\simeq G_0/\{1_G\}$，G 为单群

引理 5.3.3 $|G|<+\infty$，则 G 有合成列

证明 若 G 是单群，则 $G\geq\{1_G\}$ 为 G 的合成列；若 G 不是单群，取 $H\lhd G$ 且 $|H|$ 极大，则有 $G\geq H$，且 G/H 没有非平凡正规子群，故它是单群，对 H 继续和 G 一样的操作即可 □

例 5.25 $(\mathbb{Q},+)$ 无极大真子群

证明 假设有极大真子群 H，则 $\mathbb{Q}/H$ 没有非平凡子群，故它为 Abel 单群，故 $\mathbb{Q}/H\simeq C_p$，有满同态

$$\theta:\mathbb{Q}\longrightarrow\!\!\!\!\rightarrow C_p,\quad 1\longmapsto\overline{1}$$

则 $p\mapsto\overline{0}$，然而 $\overline{0}=\theta(p)\cdot\theta(\frac{1}{p})=\theta(p\cdot\frac{1}{p})=\overline{1}$，矛盾！

例 5.26 $D_8=<x,y|x^4=1=y^2,yxy^{-1}=x^2>$，它有两个不同的合成列

$$D_8\geq<x>\geq<x^2>\geq\{1_G\}$$

$$D_8\geq<x^2,y>\geq<y>\geq\{1_G\}$$

例 5.27 $C_6=\{g|g^6=1\}$，它有两个合成列

$$C_6\geq<g^2>\geq\{1_G\}$$

$$C_6\geq<g^3>\geq\{1_G\}$$

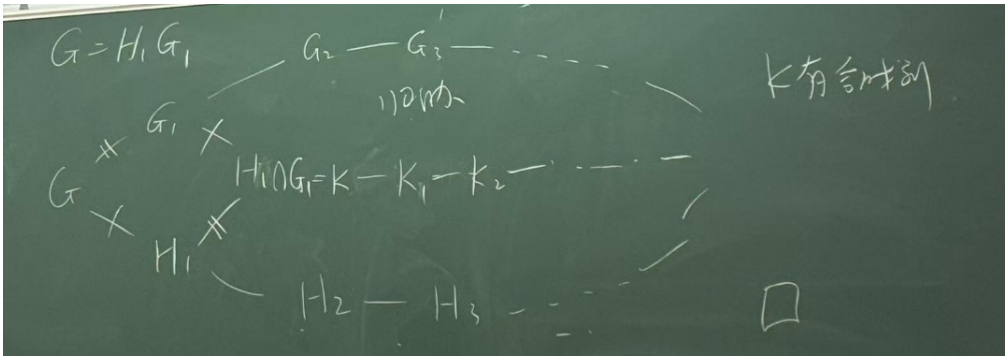
定理 5.3.3（Jordan – Holder）设 G 有两个合成列

$$G=G_0\geq G_1\geq G_2\geq\cdots\geq G_n=\{1_G\},\quad G=H_0\geq H_1\geq H_2\geq\cdots\geq H_m=\{1_G\}$$

则 $n=m$，且因子集相同

评价 能观察到不同中的相同，这就是慧眼

证明 哎，摆了



□

命题 5.3.3 设 G 是有限群，则 G 可解 $\iff$ G 的合成因子都是 C_p, p 是素数

接下来两个结论了解即可，不要求掌握

推论 5.3.1（Burnside, 1904）设 $|G| = p^a q^b, p, q$ 为素数，则 G 可解

推论 5.3.2（Feit – Thompson, 1963） $|G|$ 是奇阶群，则 G 可解

定义 5.3.5（换位子、换位子群）设 G 是群，$g, h \in G$，定义

$$[g,h] = ghg^{-1}h^{-1}$$

为 g, h 的换位子，显然有 $[g,h] = 1_G \iff gh = hg$，称

$$[G,G] = \{[g,h] : g, h \in G\}$$

为由换位子生成的子群，称为 G 的换位子群

Fact 换位子群有如下性质

(1) $[G,G] \lhd G$

(2) $G/[G,G] \overset{\text{def}}{=} G^{\text{ab}}$ 是 Abel 群

(3) 若 $N \lhd G$，则 G/N 是 Abel 群 $\iff N \supseteq [G,G]$

证明 (1).$g[a,b]g^{-1} = [gag^{-1}, gbg^{-1}] \Longrightarrow g[G,G]g^{-1} = [G,G]$ □

Fact 若 $G =< x_1, \cdots, x_n | r_1, \cdots, r_m >$，则

$$G^{\text{ab}} =< x_1, \cdots, x_n | r_1, \cdots, r_m, x_i x_j x_i^{-1} x_j^{-1}, \forall 1 \le i, j \le n >$$

定理 5.3.4 定义 $G^{(1)} = [G,G], G^{(2)} = [G^{(1)}, G^{(1)}], \cdots$，则 G 可解 $\iff \exists n \in \mathbb{N}^*, \text{s.t. } G^{(n)} = \{1_G\}$

§5.4 判别式

但遗憾的是这节课我翘了